TREND MICRO™

Remote Manager

Guida dell'utente

Codice documento: APIM36399/140410

Data di pubblicazione: aprile 2014

Protetto dal brevetto USA n.: Brevetti in sospeso.

La presente documentazione contiene l'introduzione alle caratteristiche principali del prodotto/servizio e/o le istruzioni per l'installazione in un ambiente di produzione. Leggere l'intera documentazione prima di installare o utilizzare il prodotto/servizio.

Le informazioni dettagliate su come utilizzare funzioni specifiche del prodotto/servizio sono disponibili nel Centro assistenza online di Trend Micro e/o nella Knowledge Base di Trend Micro.

Trend Micro cerca sempre di migliorare la documentazione. Per domande, commenti o suggerimenti riguardanti questo o qualsiasi documento Trend Micro, scrivere all'indirizzo docs@trendmicro.com.

È possibile esprimere un giudizio su questa documentazione al seguente indirizzo:

http://www.trendmicro.com/download/documentation/rating.asp

Sommario

Prefazione

Capitolo 1: Introduzione

Capitolo 2: Guida introduttiva

Capitolo 3: Descrizione della console Web

Capitolo 4: Preparazione dell'infrastruttura

Capitolo 5: Gestione dei clienti

Capitolo 6: Gestione degli Agent

Capitolo 7: Gestione delle licenze

Capitolo 8: Gestione delle impostazioni

Capitolo 9: Gestione degli eventi

Capitolo 10: Rapporti

Capitolo 11: Risoluzione dei problemi e problemi noti

Capitolo 12: Assistenza

Indice

Prefazione

Prefazione

Nella Guida dell'utente di Remote Manager™ sono contenute informazioni dettagliate su come utilizzare la piattaforma ed eseguire operazioni di base.

Gli argomenti includono:

Informazioni su Trend Micro

Leader globale nell'ambito della sicurezza cloud, Trend Micro sviluppa soluzioni per la protezione dei contenuti Internet e di gestione delle minacce affinché aziende e consumatori di tutto il mondo possano scambiare informazioni in modo del tutto sicuro. Con oltre 20 anni di esperienza, Trend Micro offre le migliori soluzioni client, server e basate su cloud, in grado di bloccare rapidamente le minacce e proteggere i dati in ambienti fisici, virtualizzati e cloud.

Con l'avanzare di nuove minacce e vulnerabilità, Trend Micro continua a impegnarsi per garantire ai propri clienti la sicurezza dei dati, conformità, costi ridotti e salvaguardia dell'integrità aziendale. Per ulteriori informazioni, visitare:

http://www.trendmicro.com

Pubblico

La Guida dell'utente di Trend Micro Remote Manager si rivolge ai partner e ai fornitori di servizi gestiti (MSP, managed service providers) che utilizzano la piattaforma per controllare e gestire l'intero portafoglio di prodotti Trend Micro SMB per tutti i clienti di un partner, da qualsiasi postazione e in qualsiasi momento.

Convenzioni del documento

La Guida dell'utente di Remote Manager™ si attiene alle convenzioni riportate di seguito.

Tabella 1. Convenzioni del documento

Convenzione	Descrizione
TUTTO MAIUSCOLO	Acronimi, abbreviazioni e nomi di alcuni comandi e tasti della tastiera
Grassetto	Menu e comandi dei menu, pulsanti dei comandi, schede e opzioni
Percorso di > **navigazione**	Percorso di navigazione per raggiungere una determinata schermata Ad esempio, **File** > **Salva** significa fare clic su **File**, quindi su **Salva** nell'interfaccia
Nota	Note alla configurazione
Suggerimento	Consigli o suggerimenti
AVVERTENZA!	Azioni critiche e opzioni di configurazione

Capitolo 1

Introduzione

In questa sezione sono trattati i seguenti argomenti:

Trend Micro™ Remote Manager™

Trend Micro™ Remote Manager™ è una solida console che opera in parallelo con Trend Micro Licensing Management Platform™ per fornire servizi di sicurezza gestiti alle aziende di piccole e medie dimensioni.

Remote Manager consente di monitorare lo stato di diverse reti gestite mediante più prodotti e servizi gestiti. Trend Micro Remote Manager consente agli amministratori dei rivenditori di eseguire comandi per gestire gli aspetti critici della sicurezza di rete.

Remote Manager è in hosting sui server dei data center Trend Micro dell'area geografica in cui i rivenditori ottengono un account. I rivenditori possono utilizzare Remote Manager per creare account per i clienti, monitorare le reti dei clienti e gestire la sicurezza con la console Web Remote Manager.

Remote Manager esegue il monitoraggio dei seguenti prodotti:

- Worry-Free Business Security™ Standard (in precedenza Client Server Suite) versioni 6.x, 7.x, 8.x, 9.0
- Worry-Free Business Security Advanced (in precedenza Client Server Messaging Suite) versioni 6.x, 7.x, 8.x, 9.0
- Worry-Free Business Security Services versione 5.0, 5.1, 5.2, 5.3, 5.3 SP1

Nota

Worry-Free Business Security Standard e Advanced e Worry-Free Business Security Services vengono denominati collettivamente Worry-Free Business Security (tutti), quando opportuno.

- Trend Micro Hosted Email Security™ versione 1.x

Nota

Worry-Free Business Security Standard e Advanced, Worry-Free Business Security Services e Hosted Email Security vengono denominati collettivamente "prodotti gestiti" e/o "servizi gestiti" in questo documento.

Remote Manager dispone di un pannello di controllo per il monitoraggio che consente ai rivenditori di visionare i seguenti aspetti della sicurezza di rete:

- Worry-Free Business Security (tutti):
  - Incidenti legati a virus, virus di rete, spyware/grayware
  - Incidenti legati a spam e phishing
  - Modifiche non autorizzate al computer
  - Situazioni di infezione
  - Stato di licenze e aggiornamenti dei prodotti di protezione
  - Uso del disco su computer desktop, server e server Exchange (solo Worry-Free Business Security Standard e Advanced)
  - Principali indicatori di sicurezza
- Hosted Email Security:
  - Traffico messaggi e-mail
  - Dimensioni messaggi e-mail accettati
  - Riepilogo delle minacce
  - Destinatari principali dello spam
  - Destinatari principali dei virus

Nota

Per informazioni dettagliate su Hosted Email Security e Worry-Free Business Security (tutti), consultare la rispettiva documentazione disponibile nel sito: http://docs.trendmicro.com/it-it/home.aspx.

Remote Manager offre una visione strutturata delle reti dei clienti e consente ai rivenditori di impartire comandi e gestire i seguenti aspetti cruciali della sicurezza di rete:

- Aggiornamenti dei componenti e aggiornamenti del server gestito
- Valutazione delle vulnerabilità
- Riparazione dei danni
- Risposta automatica alle infezioni

- Impostazioni del firewall e scansione in tempo reale
- Scansioni manuali

Remote Manager supporta inoltre funzionalità complete per i rapporti e consente ai rivenditori di iscrivere i clienti alla ricezione di rapporti generati automaticamente.

Caratteristiche

Trend Micro Remote Manager mette a disposizione le seguenti funzionalità.

Piattaforma integrata

Remote Manager opera in parallelo con Trend Micro™ Licensing Management Platform, ma presenta un'interfaccia più efficiente. Nel portale Remote Manager è possibile eseguire le seguenti operazioni:

- Creazione di nuovi account
- Rinnovo delle licenze per singoli account
- Aggiunta di ulteriori postazioni

Remote Manager, inoltre, monitora e gestisce diverse reti protette da una singola console mediante la comunicazione con un Agent Remote Manager eseguito sui server gestiti. Infine, Remote Manager offre il monitoraggio degli eventi basato sui principali indicatori di sicurezza.

Widget del pannello di controllo

Nella pagina del pannello di controllo, personalizzare i widget, che consentono di sapere se è necessario rinnovare le licenze, aggiungere altre postazioni allocate o addirittura quali clienti sono più esposti alle minacce.

Impostazioni personalizzabili per i nuovi account

Durante la creazione degli account, è possibile personalizzare le impostazioni predefinite di base che i nuovi account utilizzano per impostazione predefinita oppure selezionare le impostazioni da modelli precedentemente configurati e salvati.

Stato della minaccia

La schermata degli eventi di Remote Manager mostra lo stato dei seguenti aspetti della sicurezza di rete:

- Worry-Free Business Security Standard e Advanced
  - Difesa dalle infezioni
  - Antivirus
  - Anti-spyware
  - Reputazione Web
  - Monitoraggio del comportamento
  - Virus di rete
  - Anti-spam
  - Filtri URL (solo per versioni 6.x e successive)
  - Controllo dispositivi (solo nelle versioni 7.x, 8.x e 9.0)
- Worry-Free Business Security Services
  - Difesa dalle infezioni
  - Antivirus
  - Anti-spyware
  - Reputazione Web
  - Monitoraggio del comportamento
  - Virus di rete

- Filtri URL
- Hosted Email Security
    - Totale traffico messaggi e-mail
    - Dimensioni messaggi e-mail accettati
    - Riepilogo delle minacce
    - Destinatari principali dello spam
    - Destinatari principali dei virus

Remote Manager fornisce i dettagli di questi aspetti, comprensivi di dati statistici quali il numero di computer infetti e gli incidenti legati a virus/minacce informatiche. Gli amministratori dei rivenditori possono inoltre visionare informazioni dettagliate, ad esempio i nomi dei computer colpiti o delle minacce.

Stato del sistema

Gli amministratori dei rivenditori possono esaminare, mediante la schermata degli eventi di Remote Manager, i seguenti aspetti legati al sistema della sicurezza di rete:

- Smart Protection Services
- Aggiornamenti componenti
- Spazio su disco insufficiente
- Dispositivo/agente offline
- Dispositivo/agente offline (ultime 24 ore)
- Malfunzionamento del dispositivo
- Malfunzionamento del dispositivo (ultime 24 ore)

Stato licenza

Gli amministratori dei rivenditori possono visualizzare i seguenti dettagli relativi alla licenza:

- Totale postazioni acquistate
- Totale postazioni in uso
- Licenze scadute, inclusa la data di scadenza
- Licenze in scadenza, incluso il numero di giorni prima della scadenza

Gestione della rete

Remote Manager offre una visione strutturata delle reti gestite e consente agli amministratori dei rivenditori di impartire comandi e gestire i seguenti aspetti cruciali della sicurezza di rete:

- Aggiornamenti dei componenti e aggiornamenti del server gestito
- Valutazione delle vulnerabilità
- Risposta automatica alle infezioni
- Riparazione dei danni
- Impostazioni del firewall e scansione in tempo reale
- Scansioni manuali

Rapporti

Oltre alle notifiche per gli eventi legati alla sicurezza, Remote Manager può generare e inviare automaticamente rapporti a intervalli regolari. È possibile creare i rapporti in base a cliente, prodotto, frequenza e contenuto e salvarli in vari formati.

Integrazione con strumenti di terzi

Per standardizzare operazioni e processi monitorati, attivare il monitoraggio dei registri utilizzando strumenti di terzi, come Autotask™, Kaseya™ o ConnectWise™.

Invio del feedback

Trend Micro desidera offrire agli utenti la piattaforma migliore e più funzionale. Per questo motivo è importante conoscere quali servizi o funzioni sono ritenuti importanti dai clienti. A tal fine, è possibile inviare feedback e suggerimenti a Remote Manager mediante il pulsante **Invia feedback**, accessibile e visibile dal banner. Una volta vagliate le varie proposte, Trend Micro può stabilire quali funzioni soddisferebbero il maggior numero di utenti.

Prodotti supportati

- Worry-Free Business Security Standard
- Worry-Free Business Security Advanced
- Worry-Free Business Security Services
- Hosted Email Security
- Cloud Edge

Nota

Worry-Free Business Security Standard e Advanced e Worry-Free Business Security Services vengono denominati collettivamente Worry-Free Business Security (tutti), quando opportuno.

- Strumenti di terzi
    - Autotask™
    - Kaseya™
    - ConnectWise™

Worry-Free Business Security Suite

Trend Micro™ Worry-Free Business Security Standard, Worry-Free Business Security Advanced e Worry-Free Business Security Services sono soluzioni complete e gestite in modo centralizzato per aziende di piccole e medie dimensioni.

Worry-Free Business Security Standard fornisce la protezione antivirus e un firewall sul lato client per desktop e server. Worry-Free Business Security Advanced offre le stesse funzioni di Worry-Free Business Security Standard, con in più una soluzione anti-spam e contro le minacce e-mail per i server di posta sui quali viene eseguito Microsoft™ Exchange Server. Worry-Free Business Security Standard e Advanced includono un componente lato server per il monitoraggio e la gestione della protezione del client da una posizione centrale.

Worry-Free Business Security Services offre la maggior parte dei vantaggi di Worry-Free Business Security Standard. Inoltre, poiché Worry-Free Business Security Services è un servizio in hosting, è possibile gestire la sicurezza in modo centralizzato da qualsiasi posizione senza la necessità di aggiungere, installare, configurare o gestire un server. Gli esperti della sicurezza Trend Micro ospitano ed effettuano gli aggiornamenti del servizio in maniera costante.

Nota

Per informazioni su Worry-Free Business Security Standard e Advanced e Worry-Free Business Security Services, fare riferimento alla documentazione disponibile all'indirizzo:

http://docs.trendmicro.com/it-it/home.aspx

Trend Micro Remote Manager esegue il monitoraggio e la gestione delle reti protette da Worry-Free Business Security Standard e Advanced comunicando con un Agent in esecuzione sui server Worry-Free Business Security Standard e Advanced o Worry-Free Business Security Services situati nei data center Trend Micro.

Hosted Email Security

Trend Micro™ Hosted Email Security consente di bloccare spam, virus, phishing e altre minacce e-mail prima che raggiungano la rete. Essendo una soluzione in hosting, non richiede installazione e manutenzione di hardware o software e permette di recuperare il

tempo del personale IT, la produttività dell'utente, l'ampiezza di banda e la capacità di memorizzazione del server di posta e della CPU.

Inoltre, il team internazionale di esperti di Trend Micro gestisce gli hotfix, le patch, gli aggiornamenti e le regolazioni delle applicazioni, per una soluzione dalle prestazioni sempre ottimizzate.

Nota

Per informazioni su Hosted Email Security, fare riferimento alla documentazione disponibile all'indirizzo:

http://docs.trendmicro.com/it-it/home.aspx

Trend Micro Remote Manager segue il monitoraggio e la gestione delle reti protette da Hosted Email Security comunicando con il server Hosted Email Security situato nei data center Trend Micro.

Strumenti di terzi

Trend Micro Remote Manager si integra con strumenti di terzi per garantire un ambiente di rete più sicuro. Tali strumenti includono:

Autotask™

Con Remote Manager è possibile inviare le seguenti notifiche degli eventi al sistema Autotask:

- Worry-Free Business Security Standard e Advanced
  - Agent anomalo
  - Difesa dalle infezioni
  - Antivirus
  - Anti-spyware
  - Reputazione Web

- Monitoraggio del comportamento
    - Virus di rete
    - Anti-spam
    - Server gestiti non aggiornati
    - Eventi di sistema insoliti
    - Scadenza della licenza
    - Filtri URL
    - Controllo dispositivi
    - Arresto del server Worry-Free Business Security Standard e Advanced
    - Arresto server Exchange
- Worry-Free Business Security Services
    - Agent anomalo
    - Difesa dalle infezioni
    - Antivirus
    - Anti-spyware
    - Reputazione Web
    - Monitoraggio del comportamento
    - Virus di rete
    - Server gestiti non aggiornati
    - Eventi di sistema insoliti
    - Scadenza della licenza
    - Filtri URL
    - Arresto server Exchange

Questi eventi vengono inviati a Autotask nella forma di messaggi e-mail, trasformati in un ticket Autotask. Per far sì che si verifichi questa condizione, è necessario aggiungere i destinatari delle notifiche alla console Web Remote Manager e alcuni campi al sistema di ticketing Autotask. Per ulteriori informazioni, fare riferimento a *Integrazione di Autotask™ a pagina 4-16*.

Kaseya™

Con Remote Manager e Worry-Free Business Security Services è possibile inviare notifiche degli eventi al sistema Kaseya. I seguenti eventi possono essere inviati a Kaseya:

- Worry-Free Business Security Standard e Advanced
  - Agent anomalo
  - Difesa dalle infezioni
  - Antivirus
  - Anti-spyware
  - Reputazione Web
  - Monitoraggio del comportamento
  - Virus di rete
  - Anti-spam
  - Server gestiti non aggiornati
  - Eventi di sistema insoliti
  - Scadenza della licenza
  - Filtri URL
  - Controllo dispositivi
  - Arresto del server Client Server Messaging/Worry-Free Business Security Standard e Advanced
  - Arresto server Exchange

- Worry-Free Business Security Services
    - Agent anomalo
    - Difesa dalle infezioni
    - Antivirus
    - Anti-spyware
    - Reputazione Web
    - Monitoraggio del comportamento
    - Virus di rete
    - Server gestiti non aggiornati
    - Eventi di sistema insoliti
    - Scadenza della licenza
    - Filtri URL
    - Arresto server Exchange

Questi eventi vengono inviati a Kaseya nella forma di messaggi e-mail, trasformati in un ticket Kaseya. Per far sì che si verifichi questa condizione, è necessario aggiungere i destinatari delle notifiche alla console Web Remote Manager e impostare alcuni campi nel sistema di ticketing Kaseya. Per ulteriori informazioni, fare riferimento a *Integrazione di Kaseya™ a pagina 4-23*.

ConnectWise™

Con Remote Manager e Worry-Free Business Security Services è possibile inviare notifiche degli eventi al sistema ConnectWise. I seguenti eventi possono essere inviati a ConnectWise:

- Worry-Free Business Security Standard e Advanced
    - Agent anomalo
    - Difesa dalle infezioni

- Antivirus
  - Anti-spyware
  - Reputazione Web
  - Monitoraggio del comportamento
  - Virus di rete
  - Anti-spam
  - Server gestiti non aggiornati
  - Eventi di sistema insoliti
  - Scadenza della licenza
  - Filtri URL
  - Controllo dispositivi
  - Arresto del server Client Server Messaging/Worry-Free Business Security Standard e Advanced
  - Arresto server Exchange
- Worry-Free Business Security Services
  - Agent anomalo
  - Difesa dalle infezioni
  - Antivirus
  - Anti-spyware
  - Reputazione Web
  - Monitoraggio del comportamento
  - Virus di rete
  - Server gestiti non aggiornati
  - Eventi di sistema insoliti

- Scadenza della licenza
- Filtri URL
- Arresto server Exchange

Questi eventi vengono inviati a ConnectWise nella forma di messaggi e-mail, dove vengono registrati. Per far sì che si verifichi questa condizione, è necessario aggiungere i destinatari delle notifiche alla console Web Remote Manager e impostare alcuni campi nel sistema di ticketing ConnectWise. Per ulteriori informazioni, fare riferimento a *Integrazione di ConnectWise™ a pagina 4-30*.

Novità

Trend Micro™ Remote Manager comprende le nuove funzionalità e miglioramenti indicati di seguito:

FUNZIONE/MIGLIORAMENTO	DETTAGLI
Notifica azionabile	Fare clic sui collegamenti nei widget o le notifiche e-mail per visualizzare e intervenire sulle licenze che richiedono un'azione immediata o molto rapida. Se si fa clic sugli eventi, è possibile aprire anche la console Web di alcuni prodotti. Consultare Accesso singolo.
Personalizza i rapporti	Partner e clienti hanno esigenze diverse in termini di ricezione di rapporti. È possibile utilizzare nuovi contenuti e modelli per accertarsi che ricevano le informazioni corrette.

FUNZIONE/MIGLIORAMENTO	DETTAGLI
Imposta nuovo cliente in 3 semplici passi **Nota** Questa funzione è disponibile solo per gli utenti di Trend Micro Licensing Management Platform. Per ulteriori informazioni, contattare il fornitore del servizio gestito o il rappresentante Trend Micro.	Impostare e implementare i criteri predefiniti per i nuovi clienti in tre (3) passaggi. Successivamente, tali clienti disporranno dello stesso livello di protezione e monitoraggio da Trend Micro Remote Manager.
Personalizza modelli impostazione predefinita **Nota** Questa funzione è disponibile solo per gli utenti di Trend Micro Licensing Management Platform. Per ulteriori informazioni, contattare il fornitore del servizio gestito o il rappresentante Trend Micro.	Preconfigurare diversi modelli per le impostazioni Worry-Free Business Security Services. Ciò consente di adattarsi con flessibilità a diversi modelli di servizio per i clienti.
Accesso singolo	Dalla pagina Cliente, fare clic sul collegamento **Apri console** per aprire la console Web dei seguenti servizi: • Worry-Free Business Security Services • Hosted Email Security • Cloud Edge

Funzione/Miglioramento	Dettagli
Assistenza aggiuntiva	Trend Micro Remote Manager offre un rapido accesso alla documentazione mediante il pulsante **Guida**, che include anche tutorial video visualizzabili direttamente dalla console. Trend Micro Remote Manager fornisce inoltre un collegamento rapido alla guida con le best practice di Trend Micro Remote Manager.

Infrastruttura generale

Trend Micro Remote Manager è costituito da tre parti fondamentali:

- Il rivenditore
- Il data center Trend Micro
- La rete del cliente

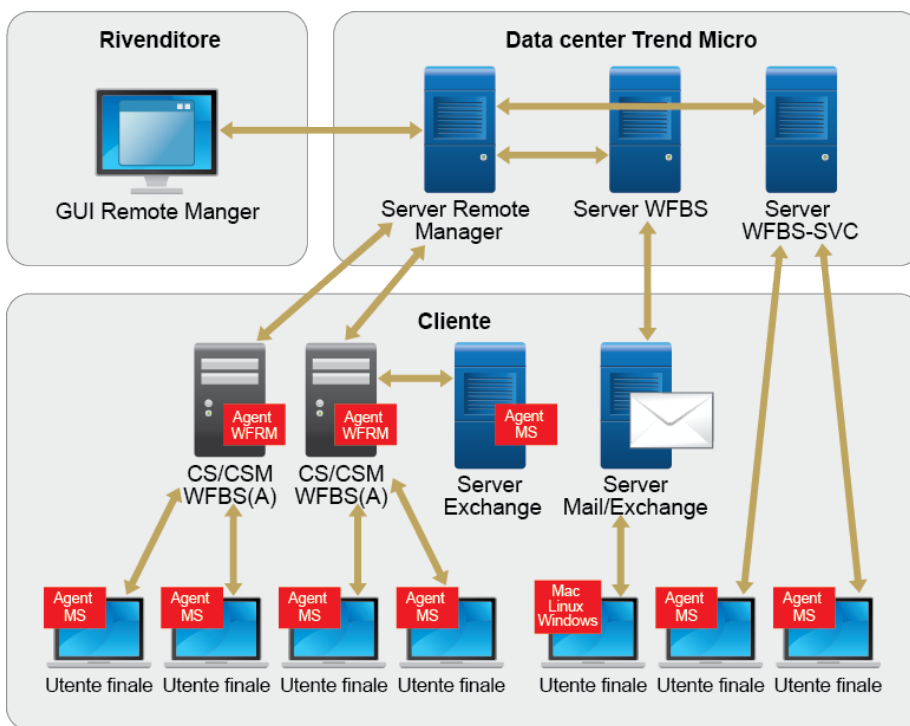



FIGURA 1-1. Architettura complessiva di Remote Manager

Il rivenditore accede a un data center Trend Micro (attualmente presenti in diversi continenti) mediante la console Web Remote Manager tramite Internet. Il rivenditore non deve installare alcun componente per poter utilizzare il prodotto. È sufficiente che aggiunga e configuri ciascun cliente sulla console Web Remote Manager prima di gestire gli account dei clienti.

Ciascun server gestito Worry-Free Business Security Standard e Advanced dispone di un Agent Remote Manager installato che permette la comunicazione da e verso i server Remote Manager. Poiché Worry-Free Business Security Services è ospitato nel data center Trend Micro, non è necessario installare alcun Agent. Worry-Free Business Security Services deve invece essere registrato sulla console Web Remote Manager per ogni cliente.

L'Agent Remote Manager, che può essere installato dalla console Web Remote Manager, viene eseguito sul server gestito Worry-Free Business Security Standard e Advanced all'interno della rete del cliente. L'Agent Remote Manager invia informazioni al server Remote Manager dove è possibile accedere ai dati dalla console in qualsiasi momento, utilizzando una connessione a Internet.

Terminologia di base

La conoscenza della seguente terminologia può consentire un uso più efficiente di Remote Manager:

TERMINE	DEFINIZIONE
Agent	Installato sui server Worry-Free Business Security Standard e Advanced, questo programma consente a Remote Manager di monitorare e gestire Worry-Free Business Security Standard e Advanced.
Valutazione	Controlli regolari eseguiti sui dati raccolti dalle reti dei clienti per determinare lo stato delle reti monitorate. Questi controlli utilizzano indicatori chiave chiamati indici di valutazione.
Indici di valutazione	La base delle valutazioni di sicurezza. Gli amministratori dei rivenditori possono personalizzare questi indici per controllare gli intervalli di valutazione, gli intervalli e le notifiche.
Client Security Agent (CSA)	L'Agent che fa riferimento al server Worry-Free Business Security. CSA invia le informazioni sullo stato degli eventi in tempo reale. Gli eventi riportati sono ad esempio il rilevamento delle minacce, l'avvio e l'arresto dell'Agent, l'avvio di una scansione e il completamento di un aggiornamento. CSA mette a disposizione tre metodi di scansione: in tempo reale, pianificata e manuale. È possibile configurare le impostazioni di scansione sugli Agent dalla console Web.
Pannello di controllo	Il pannello di controllo di Remote Manager è la schermata principale (scheda **Home**) sulla quale sono visualizzati la console Web e i widget.

TERMINE	DEFINIZIONE
Rilevamento	Il rilevamento di una minaccia; un rilevamento non costituisce un'infezione del sistema, ma indica semplicemente che la minaccia informatica ha raggiunto il computer. Il rilevamento della stessa minaccia su computer differenti può costituire un'infezione.
Evento	Gli eventi segnalano il verificarsi di una condizione in un dominio monitorato.
Globally Unique Identifier (GUID) o chiave di autorizzazione	Un numero di riferimento univoco utilizzato come identificatore nel software del computer.
Infezione	La condizione in cui una minaccia è in grado di liberare la sua carica distruttiva in un computer; Remote Manager stabilisce che si è verificata un'infezione quando il sistema di scansione antivirus rileva un virus o una minaccia informatica e non è in grado di disinfettare, eliminare o mettere in quarantena tale minaccia. Un'infezione da spyware/grayware si verifica quando il computer non può essere completamente disinfettato senza riavviarlo.
Messaging Security Agent (MSA)	L'Agent che risiede sui server Microsoft Exchange e fa riferimento ai server Client Server Messaging e Worry-Free Business Security Advanced. Questo Agent protegge da virus/ minacce informatiche, cavalli di Troia, worm e altre minacce veicolate via e-mail. Fornisce inoltre blocco dello spam, filtro dei contenuti e blocco degli allegati.
Rivenditore	Termine generico per fare riferimento a organizzazioni che forniscono direttamente servizi di monitoraggio e gestione della sicurezza ai clienti in Remote Manager.
Amministratori dei rivenditori	Amministratori sul lato del rivenditore che eseguono operazioni correlate ai servizi utilizzando Remote Manager.
Data center Trend Micro	Il centro di monitoraggio e gestione Trend Micro in cui risiedono i server Remote Manager (e Hosted Email Security) e che fornisce assistenza agli amministratori dei rivenditori.
Security Server	Il computer server Worry-Free Business Security Standard e Advanced.

Termine	Definizione
Avviso virus	Uno stato di allerta dichiarato da TrendLabs℠ per preparare le reti dei clienti a un'infezione virale; TrendLabs avvisa diversi prodotti Trend Micro e consegna soluzioni preventive che gli amministratori IT possono implementare come prima linea di difesa prima che diventi disponibile un pattern.
Infezione virale	La propagazione rapida di un virus su diversi computer e reti. In base alla prevalenza della minaccia, un'infezione può essere interna, zonale o globale.

Capitolo 2

Guida introduttiva

In questa sezione sono trattati i seguenti argomenti:

Requisiti del browser

- Connessione a Internet
- Informazioni sull'account Remote Manager da Trend Micro
- Browser supportati:
    - Versione più recente di Firefox™ (consigliata)
    - Versione più recente di Google™ Chrome™ (consigliata)
    - Internet Explorer™ 9.0

Aggiunta dell'URL della console Web Trend Micro Remote Manager ai siti attendibili

Aggiungere l'URL della console Web Remote Manager all'elenco di siti attendibili in Internet Explorer per garantire la possibilità di accesso a tutte le schermate e a tutte le funzionalità della console in modo corretto.

Procedura

1. Aprire Internet Explorer.
2. Fare clic su **Strumenti** > **Opzioni Internet** > **Sicurezza (scheda)**.
3. Selezionare l'area **Siti attendibili**.
4. Fare clic su **Siti**.
5. In **Aggiungi il sito Web all'area**, digitare l'URL della console.
6. Fare clic su **Aggiungi**.
7. Fare clic su **OK**.

Uso di Internet Explorer 9 per ottenere il certificato SSL

Per utilizzare l'Agent, aggiungere il certificato SSL di Trend Micro al browser sul server gestito.

Procedura

1. Aprire Internet Explorer e accedere al sito Trend Micro Remote Manager corrispondente alla propria area geografica.
2. Fare doppio clic sull'icona del lucchetto a destra della barra degli indirizzi.

   Viene aperto il menu di identificazione del sito Web.
3. Fare clic su **Visualizza certificati**.

   Viene aperta la finestra Certificato in cui è visualizzato il certificato emesso per `*.trendmicro.com`.
4. Accedere a **Percorso certificazione (scheda)** > **Geotrust o Equifax Secure Certificate Authority** > **Visualizza certificato**.
5. Quando viene aperta la finestra **Certificato** in cui è visualizzata la Certificate Information Authority, fare clic sulla scheda **Dettagli**.
6. Accedere a **Copia su file** > **Avanti**, quindi selezionare **DER encoded binary X. 509 (.CER)**.
7. Fare clic su **Avanti** e immettere il percorso e il nome file del certificato.

   Ad esempio, `wfrmcert.cer`.
8. Fare clic su **Avanti** > **Fine**.

Accesso alla piattaforma

Tutti, indipendentemente dal tipo di account e dalle autorizzazioni di cui dispongono, eseguono l'accesso dalla stessa pagina. Digitare semplicemente le proprie credenziali e fare clic su **Accedi**. Si dovrebbero ottenere l'URL di accesso e le credenziali dall'utente con l'account principale.

Gli utenti non sono in grado di visualizzare le impostazioni e le opzioni per le quali sono richiesti privilegi specifici.

Coordinazione con il cliente

Il monitoraggio e la gestione della rete del cliente tramite Trend Micro Remote Manager offrono numerosi vantaggi al cliente. Tuttavia, come qualsiasi altra attività di gestione remota, le operazioni eseguite sulla console possono influire drasticamente sulla rete gestita.

Prima di iniziare a fornire servizi, assicurarsi di avere il consenso del cliente a effettuare le seguenti attività di gestione e monitoraggio remoto:

- Visualizzare l'elenco dei computer sulla rete
- Rinnovare o aggiornare le postazioni nelle licenze
- Visualizzare le seguenti informazioni sulla sicurezza:
    - Rilevamenti di virus/minacce informatiche, spyware/grayware e virus di rete
    - Nomi e numero dei computer infetti
    - Nomi dei file infetti
    - Indirizzi e-mail che hanno ricevuto file infetti
    - Informazioni sulle patch per le vulnerabilità note
    - Informazioni sulla licenza e sul sistema in Worry-Free Business Security (tutti) e Hosted Email Security
- Inviare notifiche agli individui nell'organizzazione del cliente
- Effettuare le seguenti operazioni:
    - Implementare componenti di sicurezza
    - Avviare scansioni di valutazione delle vulnerabilità
    - Avvia Damage Cleanup Services
    - Avviare o arrestare scansioni manuali

- Aggiornare il server Worry-Free Business Security Standard e Advanced
    - Avviare o arrestare Outbreak Defense
- Configurare le seguenti impostazioni:
    - Implementazione automatica della difesa dalle infezioni
    - Impostazioni scansione in tempo reale
    - Impostazioni del firewall
    - Location Awareness
    - Monitoraggio del comportamento
    - Reputazione Web
    - Filtri URL
    - Controllo dispositivi (Worry-Free Business Security 7.0 e versioni successive)

Capitolo 3

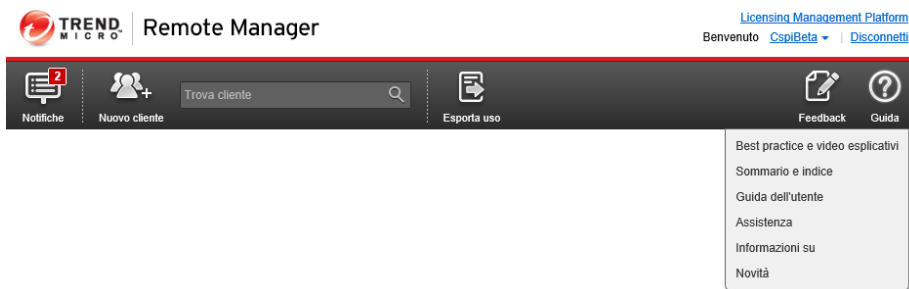
Descrizione della console Web

La console Web è il punto centrale per il monitoraggio e la gestione dei prodotti e dei clienti.

In questa sezione sono trattati i seguenti argomenti:

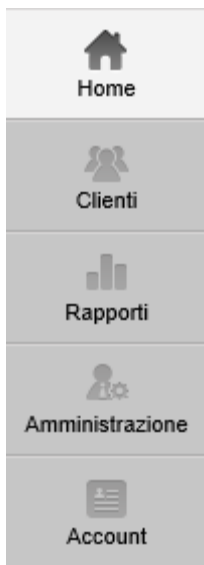
- *Banner della console Web a pagina 3-2*
- *Menu principale a pagina 3-3*
- *Informazioni sul pannello di controllo a pagina 3-4*

Banner della console Web

L'area del banner offre le seguenti opzioni:

- **<nome account>**: mostra l'account con il quale si è eseguito l'accesso.
- **Disconnetti**: con questa opzione ci si disconnette dalla console Web.
- **Licensing Management Platform**: questo collegamento viene visualizzato solo se il sito di License Management Platform è stato integrato.
- **Notifiche**: indica il numero di eventi che richiedono un'azione.
- **Nuovo cliente**: fare clic su questo pulsante per aggiungere un nuovo cliente.
- **Barra di ricerca**: consente di inserire le informazioni su un cliente specifico per ricercarlo.
- **Esporta uso**: fare clic su questo pulsante per esportare un documento relativo all'uso della licenza.
- **Feedback**: fare clic su questo pulsante per inviare un utile feedback a Trend Micro inerente all'uso del prodotto e alle funzioni che si ritiene debbano essere aggiunte o a come rendere più funzionali le attuali funzioni.
- **Guida**:
    - **Best practice e video esplicativi**: apre la pagina in cui è possibile guardare i video esplicativi e fornisce un collegamento alla guida alle best practice.

- **Sommario e indice**: apre la Guida in linea di Trend Micro Remote Manager.
- **Guida dell'utente**: consente di scaricare e visualizzare la Guida dell'utente in formato PDF.
- **Assistenza**: visualizza la pagina Web relativa all'assistenza Trend Micro, in cui è possibile inviare domande e trovare risposte a quesiti comuni inerenti ai prodotti Trend Micro.
- **Informazioni su**: offre una panoramica del prodotto e le istruzioni per verificare i dettagli della versione dei componenti.
- **Novità**: collega alla pagina in cui è possibile informarsi sulle nuove funzioni.

Menu principale

Nel menu principale sono visualizzati i pulsanti relativi a funzioni e opzioni. Dalla barra di navigazione è possibile fare clic sulle seguenti opzioni:

- **Home**: viene visualizzata la homepage che contiene il pannello di controllo e i widget sul riquadro a destra.
- **Clienti**: viene visualizzato un elenco di clienti in cui è possibile aggiungere clienti o apportare modifiche alle impostazioni o alle configurazioni dei clienti.
- **Rapporti**: vengono visualizzati e rapporti esistenti e quelli nuovi che è possibile aggiungere.
- **Amministrazione**: È la pagina in cui si possono modificare le impostazioni della console Web o delle notifiche, i modelli di impostazione predefinita oppure configurare l'integrazione con strumenti di terzi.
- **Account**: questa pagina viene visualizzata solo nel caso in cui l'account non sia stato integrato con Licensing Management Platform.

Informazioni sul pannello di controllo

In questa sezione sono fornite informazioni su schede, widget e pannello di controllo.

Schermate di stato del pannello di controllo

Il pannello di controllo è la schermata principale che consente di visionare lo stato delle reti monitorate. Nel pannello di controllo sono elencati solo i prodotti con stato non normale. Ad esempio, vi figurano soli i clienti la cui licenza Worry-Free Business Security Services sta per scadere o con un numero eccessivo di minacce.

Per accedere al pannello di controllo, aprire un browser compatibile e accedere al sito di Trend Micro Remote Manager relativo alla propria area geografica.

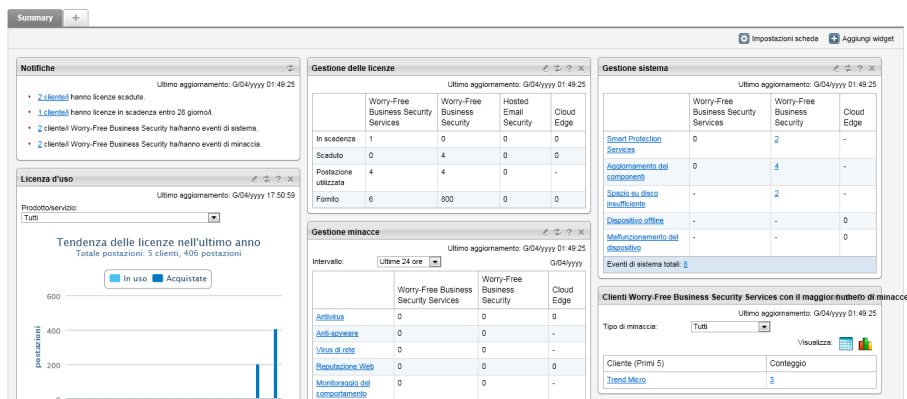



FIGURA 3-1. Scheda Stato della minaccia del pannello di controllo

Molti elementi sul pannello di controllo sono collegati per facilitare la risoluzione di un problema. Fare clic su un elemento (grafico, collegamento, numero) per risolvere il problema. Per informazioni dettagliate sulle operazioni che è possibile eseguire, consultare *Informazioni prodotto/servizio a pagina 3-19*.

Schede e widget

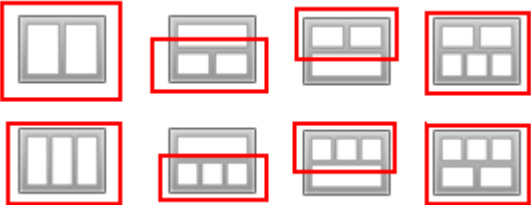
Nelle schede sono contenuti i widget. Ogni scheda nella schermata **Riepilogo** può contenere fino a 20 widget. La scheda **Riepilogo** stessa supporta fino a 30 schede.

I widget sono i componenti principali del pannello di controllo. I widget forniscono informazioni specifiche sui vari eventi correlati alla sicurezza o alle licenze. Alcuni widget consentono di eseguire determinate operazioni.

Le informazioni visualizzate in un widget provengono da:

- server e client Worry-Free Business Security
- server Worry-Free Business Security Services
- servizi Hosted Email Security

- server e client Cloud Edge

Operazioni delle schede

Nella seguente tabella sono riportate tutte le operazioni correlate alle schede:

OPERAZIONE	PASSAGGI
Aggiunta di una scheda	Fare clic sull'icona del simbolo più (+) nella parte superiore della schermata **Riepilogo**. Viene visualizzata la finestra **Nuova scheda**.
Modifica delle impostazioni della scheda	Fare clic su **Impostazioni scheda**. Viene visualizzata una finestra simile a **Nuova scheda** nella quale è possibile modificare le impostazioni.
Spostamento della scheda	Utilizzare la funzione di trascinamento per modificare la posizione di una scheda.
Eliminazione della scheda	Fare clic sull'icona Elimina ( ) accanto al titolo della scheda. Se si elimina una scheda, vengono eliminati anche tutti i widget in essa contenuti.

Operazioni dei widget

Nella seguente tabella sono riportate tutte le operazioni correlate ai widget:

OPERAZIONE	PASSAGGI
Aggiunta di un widget	Aprire una scheda, quindi fare clic su **Aggiungi widget** nell'angolo superiore destro della scheda. Viene visualizzata la schermata **Aggiungi widget**.
Aggiornamento dei dati del widget	Fare clic sull'icona Aggiorna ( ).
Visualizzazione della Guida	Fare clic su **Guida** (?).

OPERAZIONE	PASSAGGI
Eliminazione di un widget	Fare clic su **Chiudi widget** ( ). Con questa operazione il widget viene rimosso dalla scheda attiva, ma non dalle altre che lo contengono o dall'elenco dei widget nella schermata **Aggiungi widget**.
Spostamento di un widget	Utilizzare la funzione di trascinamento per spostare un widget in una posizione diversa all'interno della scheda.
Ridimensionamento di un widget	Puntare il cursore all'estremità destra di un widget per ridimensionarlo. Quando vengono visualizzate una linea spessa verticale e una freccia (come nell'immagine seguente), tenere premuto e spostare il cursore a sinistra o a destra. È possibile ridimensionare solo i widget su schede costituite da più colonne. Tali schede presentano uno dei seguenti layout e le sezioni evidenziate contengono widget ridimensionabili.

Widget disponibili

Nel pannello di controllo sono visualizzati i seguenti widget.

Widget Notifiche

Mostra gli eventi che richiedono un'azione. Possono essere eventi correlati a minacce o a licenze.

Nota

Questo widget è permanente ed è impossibile aggiungerlo o eliminarlo.

Widget Clienti che necessitano di maggiore attenzione

Mostra il numero di clienti più recente con e il maggior numero di eventi che richiedono un'azione o una risposta immediata. I dati sono visualizzati sotto forma di tabella e grafico a torta. È possibile alternare queste due modalità di visualizzazione dei dati facendo clic sulle icone visualizzate ( ).

- Se il numero di clienti per uno stato particolare è maggiore o pari a 1, è possibile fare clic sul numero per visualizzare gli eventi nella struttura del prodotto.
- Fare clic sul nome del cliente per visualizzare tutti gli eventi i rispettivi eventi o espandere il nome del cliente per visualizzare gli eventi relativi ad alcune categorie.

- Il numero di eventi presente in **Azione richiesta** corrisponde agli eventi che è opportuno gestire il prima possibile.
- Il numero di eventi presente in **Attenzione** corrisponde agli eventi non urgenti come quelli in Azione richiesta, ma che è necessario gestire rapidamente.

Widget Gestione minacce

Mostra il conteggio di eventi di minaccia per tutti i prodotti registrati.

	Worry-Free Business Security Services	Worry-Free Business Security	Cloud Edge
Antivirus	0	0	0
Anti-spyware	0	0	-
Virus di rete	0	0	-
Reputazione Web	0	97	0
Monitoraggio del comportamento	0	0	-
Filtri URL	3	408	-
Controllo dispositivi	0	0	-
Botnet	-	-	0
IPS	-	-	0

Eventi di minaccia totali: 508

- È possibile modificare l'intervallo di tempo per i dati visualizzati selezionando una delle opzioni seguenti:
  - Ultime 24 ore (predefinito)
  - Ultimi 7 giorni
  - Ultimi 30 giorni
- Se il numero di eventi per una particolare categoria è maggiore o pari a 1, è possibile fare clic sul numero per visualizzare i registri eventi.

Widget Gestione sistema

Mostra il numero attuale di tutti gli eventi di sistema per i prodotti registrati. È possibile utilizzarlo per determinare problemi hardware o eventi per il server o l'Agent.

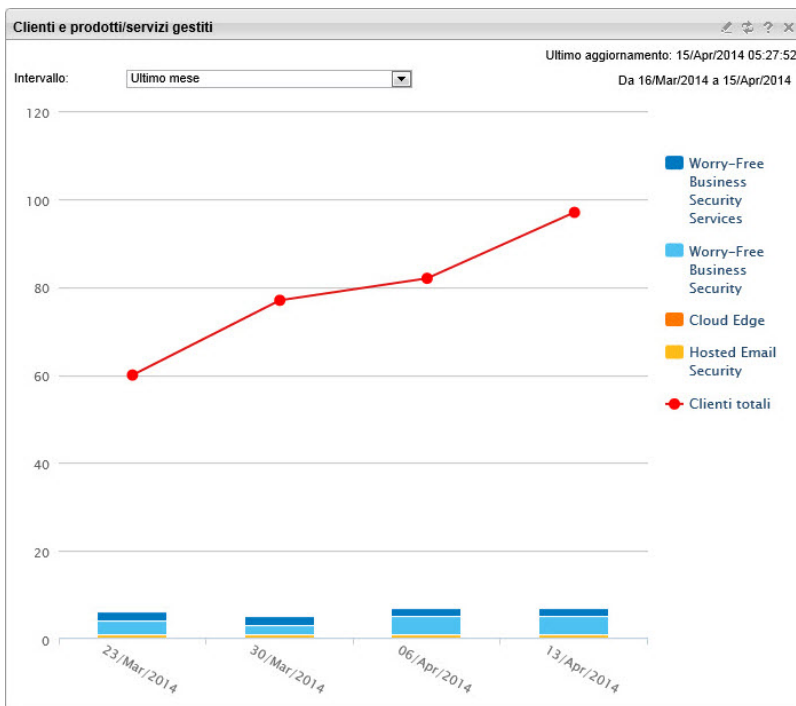
Gestione sistema

Ultimo aggiornamento: 15/Apr/2014 05:27:51

	Worry-Free Business Security Services	Worry-Free Business Security	Cloud Edge
Smart Protection Services	0	2	-
Aggiornamento dei componenti	0	4	-
Spazio su disco insufficiente	-	2	-
Dispositivo offline	-	-	0
Malfunzionamento del dispositivo	-	-	0
Eventi di sistema totali: 8			

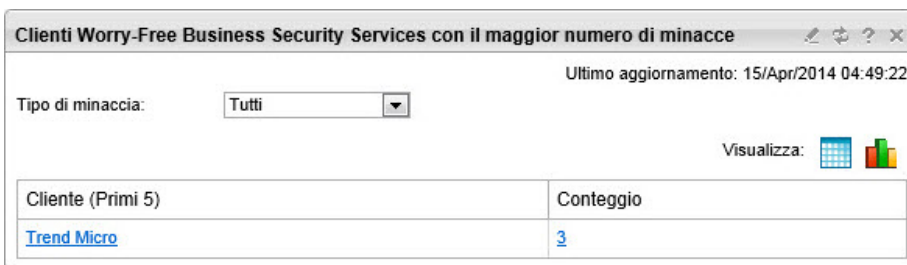
Se il numero di eventi per una particolare categoria è maggiore o pari a 1, è possibile fare clic sul numero per visualizzare i registri eventi.

Widget Clienti e prodotti/servizi gestiti

Mostra il numero di clienti gestiti per ciascun prodotto entro un determinato periodo di tempo.

- È possibile modificare l'intervallo di tempo per i dati visualizzati selezionando una delle opzioni seguenti:
  - Ultimo mese (predefinito)
  - Ultimi 3 mesi
  - Ultimi 6 mesi
  - Ultimo anno

- È possibile fare clic sui nomi dei prodotti registrati a destra per aggiungere o rimuovere dati nel grafico.
- Ogni grafico a barre rappresenta una settimana o un mese.
- Il grafico a barre mostra il numero totale di prodotti/servizi.

Widget Clienti Worry-Free Business Security Services con il maggior numero di minacce

Mostra i clienti Worry-Free Business Security Services con il numero più elevato di eventi di minaccia. I dati sono visualizzati sotto forma di tabella e grafico a torta. È possibile alternare queste due modalità di visualizzazione dei dati facendo clic sulle icone visualizzate ( ).

- È possibile modificare il tipo di minaccia per i dati visualizzati selezionando una delle opzioni seguenti:
  - Antivirus
  - Anti-spyware
  - Reputazione Web
  - Filtri URL
  - Monitoraggio del comportamento
  - Virus di rete
  - Controllo dispositivi

- Fare clic sul nome del cliente per visualizzare le informazioni corrispondenti.
- Se il numero di minacce è maggiore o pari a 1, è possibile fare clic sul numero per visualizzare i registri eventi.

Widget Clienti Cloud Edge con il maggior numero di minacce

Mostra i clienti Cloud Edge che presentano il maggior numero di eventi di minaccia. I dati sono visualizzati sotto forma di tabella e grafico a torta. È possibile alternare queste due modalità di visualizzazione dei dati facendo clic sulle icone visualizzate ( ).

- È possibile modificare l'intervallo di tempo per i dati visualizzati selezionando una delle opzioni seguenti:
    - Ultima ora
    - Ultime 24 ore (predefinito)

- Ultimi 7 giorni
    - Ultimi 30 giorni
- È possibile modificare il tipo di minaccia per i dati visualizzati selezionando una delle opzioni seguenti:
    - Tutti
    - Botnet
    - Sistema di rilevamento anti-intrusione (IPS)
    - Reputazione Web
    - Virus
- Fare clic sul nome del cliente per visualizzare le informazioni corrispondenti.
- Fare clic sul conteggio delle minacce per visualizzare le informazioni sulle minacce nella console Cloud Edge.

Widget Dispositivi Cloud Edge con maggior numero di minacce

Mostra i dispositivi Cloud Edge che presentano il maggior numero di eventi di minaccia.

- È possibile modificare l'intervallo di tempo per i dati visualizzati selezionando una delle opzioni seguenti:
  - Ultima ora
  - Ultime 24 ore (predefinito)
  - Ultimi 7 giorni
  - Ultimi 30 giorni
- È possibile modificare il tipo di minaccia per i dati visualizzati selezionando una delle opzioni seguenti:
  - Tutti
  - Botnet
  - Sistema di rilevamento anti-intrusione (IPS)
  - Reputazione Web
  - Virus
- Fare clic sul nome del cliente per visualizzare le informazioni corrispondenti.
- Fare clic sul conteggio delle minacce per visualizzare le informazioni sulle minacce nella console Cloud Edge.

Widget Gestione delle licenze

Mostra lo stato attuale delle licenze utilizzate dai clienti.

Gestione delle licenze

Ultimo aggiornamento: 15/Apr/2014 05:27:50

	Worry-Free Business Security Services	Worry-Free Business Security	Hosted Email Security	Cloud Edge
In scadenza	1	0	0	0
Scaduto	0	4	0	0
Postazione utilizzata	4	4	0	-
Fornito	6	800	0	0

Mostra i seguenti dettagli correlati alle licenze per clienti e prodotti:

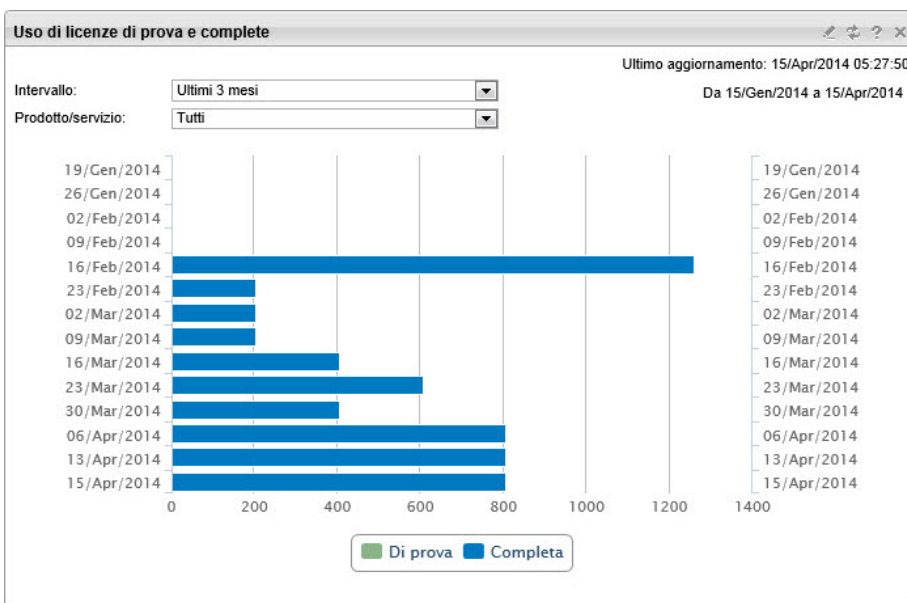
- **In scadenza**: indica il numero di licenze non ancora scadute, ma prossime alla scadenza.
- **Scaduto**: indica le licenze scadute.

Nota

Si consiglia di rinnovare queste licenze quanto prima.

- **Postazioni utilizzate**: indica il numero di postazioni attualmente utilizzate.
- **Fornito**: corrisponde al numero di postazioni fornite al cliente.

Widget Uso di licenze di prova e complete

Mostra quante licenze di prova o complete sono state utilizzate per i prodotti registrati.

È possibile modificare l'intervallo di tempo per i dati visualizzati selezionando una delle opzioni seguenti:

- Ultimo mese (predefinito)
- Ultimi 3 mesi
- Ultimi 6 mesi
- Ultimo anno

È possibile modificare il prodotto/servizio selezionando una delle seguenti opzioni:

- Tutti
- Hosted Email Security
- Worry-Free Business Security
- Worry-Free Business Security Services
- Cloud Edge

Widget Uso licenza

Visualizza un'analisi grafica delle postazioni allocate e di quelle effettivamente acquistate durante l'anno. Ciò consente di stabilire se è necessario aumentare o ridurre l'allocazione di postazioni.

È possibile modificare il prodotto/servizio selezionando una delle seguenti opzioni:

- Tutti
- Hosted Email Security
- Worry-Free Business Security
- Worry-Free Business Security Services

Informazioni prodotto/servizio

Nel pannello di controllo sono riportati solo i clienti che necessitano di attenzione. Per ottenere i dettagli sui prodotti, compresi quelli non elencati nel pannello di controllo, passare alla scheda **Clienti** e accedere al prodotto attraverso la struttura clienti.

Fare clic su **Clienti** > **{cliente}** > **{prodotto}** per visualizzare ulteriori informazioni.

Nota

le opzioni visualizzate variano in base al prodotto/servizio.

- Worry-Free Business Security Services
  - **Gruppi**: riporta i tipi e i gruppi configurati.
  - **Informazioni licenza**: visualizza tutti i dettagli della licenza.
  - **Endpoint**: riporta il nome, l'indirizzo IP, lo stato online/offline e dettagli relativi a motore di scansione, file di pattern e piattaforma.
  - **Impostazioni di sicurezza**: consente di configurare le impostazioni di sicurezza di Worry-Free Business Security Services. Per informazioni dettagliate, consultare i documenti di *Trend Micro Worry-Free Business Security Services*.

  Nota

  per apportare modifiche più particolareggiate, accedere alla console Worry-Free Business Security Services.

- Worry-Free Business Security
  - **Gruppi**: riporta i vari gruppi configurati sul server. È possibile richiedere di avviare o interrompere una scansione da qui.
  - **Endpoint**: riporta il nome, l'indirizzo IP, lo stato online/offline e dettagli relativi a motore di scansione, file di pattern e piattaforma.
  - **Informazioni licenza**: visualizza tutti i dettagli della licenza.

- **Impostazioni dominio**: consente di configurare le impostazioni per l'intero dominio. Per informazioni dettagliate, consultare i documenti di *Trend Micro Worry-Free Business Security*.

Nota

non è possibile configurare qui le impostazioni di sicurezza dei singoli gruppi. Per tali modifiche è necessario accedere alla console Worry-Free Business Security.

- **Server gestito**: visualizza tutti i dettagli del server. È possibile richiedere di aggiornare il server e gli Agent da qui.
- **Agente TMRM**: contiene informazioni generali sull'Agent Trend Micro Remote Manager, tra cui la disponibilità, il Globally Unique Identifier (GUID) o la chiave di autorizzazione e l'indirizzo IP.
- **Impostazioni di sicurezza**: consente di configurare le impostazioni di sicurezza di un gruppo particolare (applicabile solo per Worry-Free Business Security 6.0 e versioni successive). Per informazioni dettagliate, consultare i documenti di *Trend Micro Worry-Free Business Security*.

- Hosted Email Security
  - **Stato in tempo reale**: visualizza le informazioni più recenti relative a Hosted Email Security
  - **Impostazioni dei criteri**: sono riportati tutti i criteri disponibili.
  - **Mittenti approvati**: riporta tutti i mittenti approvati.
  - **Informazioni licenza**: visualizza tutti i dettagli della licenza.

Nota

per apportare modifiche più particolareggiate, accedere alla console Hosted Email Security.

Visualizzazione dei prodotti gestiti

Per visualizzare i prodotti gestiti, fare clic su **Clienti** > **{nome cliente}** > **Prodotti (scheda)**. Sul riquadro a destra di questa scheda è visualizzata una struttura dei prodotti

gestiti dei clienti e le informazioni dettagliate, le impostazioni e le possibilità di controllo sono visualizzate nel riquadro a destra.

Per informazioni dettagliate su Hosted Email Security e Worry-Free Business Security (tutti), consultare la rispettiva documentazione.

Clienti

La pagina **Clienti** fornisce una rappresentazione dei clienti e dei loro prodotti in gestione. Per impostazione predefinita, nella scheda è visualizzata una tabella di tutti i clienti. Fare clic sul nome dell'azienda per visualizzare una struttura dei relativi prodotti nel riquadro a sinistra e le informazioni dettagliate, le impostazioni e le possibilità di controllo nel riquadro a destra.

Nota

Per informazioni dettagliate su Hosted Email Security e Worry-Free Business Security (tutti), consultare la rispettiva documentazione.

Per visualizzare un prodotto nell'elenco dei clienti, fare clic su **Clienti** > **{nome cliente}** > **{prodotto}**. Sono disponibili le operazioni seguenti:

- Digitare il nome di un cliente o di un account
- Filtrare l'elenco visualizzato per cliente, prodotti, minacce, sistemi o eventi di licenza

  Nota

  Quando si filtrano gli eventi, è possibile scegliere uno, due o tutti gli eventi o prodotti contemporaneamente.

- Scorrere tutti i clienti servendosi delle frecce delle pagine.

È possibile eseguire altre operazioni:

- *Aggiunta di nuovi clienti a pagina 5-2*
- *Rinnovo delle licenze dei clienti le cui licenze stanno per scadere o sono scadute a pagina 7-2*
- *Esportazione di rapporti per clienti specifici a pagina 10-8*

Per eseguire comandi specifici, è inoltre possibile aggiungere nuovi clienti e fare clic con il pulsante destro del mouse sulla maggior parte dei nodi della struttura.

FIGURA 3-2. Elenco dei clienti

FIGURA 3-3. Struttura clienti

Struttura di rete

Sul lato sinistro della scheda **Clienti** è visualizzata una rappresentazione della struttura delle reti dei clienti. È possibile eseguire la ricerca di un cliente, visualizzare tutti i prodotti contemporaneamente oppure solo Worry-Free Business Security (tutti), Hosted Email Security o Cloud Edge nell'elenco a discesa **Visualizza per** oppure scorrere tutti i clienti mediante le frecce delle pagine. Inoltre, si può aggiungere un cliente e fare clic con il pulsante destro del mouse sulla maggior parte dei nodi della struttura per eseguire

comandi specifici. Nella tabella riportata di seguito sono descritti gli oggetti della struttura di rete.

TABELLA 3-1. Oggetti della struttura di rete

ICONA	OGGETTO DI RETE	DESCRIZIONE
	Prodotto/servizio	Il prodotto/servizio non è connesso a Remote Manager.
	Prodotto/servizio	Il prodotto/servizio è connesso a Remote Manager.
	Gruppo	Gruppo di server; questo gruppo gestisce diversi Client Security Agent (CSA).
	Gruppo	Un gruppo di desktop
	Server	Un computer server, sul quale viene eseguito Client Security Agent (CSA).
	Server Exchange	Un computer con Exchange Server e sul quale viene eseguito Messaging Security Agent (MSA).
	Desktop	Un computer desktop sul quale è eseguito Client Security Agent (CSA).

Riquadro a destra

Nel riquadro a destra è visualizzato quanto segue:

Prodotti

La scheda Prodotti nel riquadro a destra elenca tutti i prodotti di un cliente e consente di eliminarli. Per visualizzare i **prodotti**, fare clic su **Clienti** > **{nome clienti}** > **Prodotti (scheda)**. Per eliminare un prodotto, selezionare l'icona a sinistra del prodotto e fare clic su **Elimina**. Di seguito sono elencate le voci di interfaccia della scheda **Prodotti**:

- Nome prodotto
- Tipo di prodotto
- Categoria
- Incidenti

- Dettagli
- Stato

Nota

L'aggiornamento dei nuovi dati di Hosted Email Security sulla console Web Remote Manager può richiedere un massimo di tre ore. Le informazioni sui clienti Hosted Email Security vengono aggiornate una volta al giorno. Vedere *Aggiornamento di dati e impostazioni di Hosted Email Security a pagina 3-31*.

Licenze

La scheda **Licenze** di un cliente contiene tutte le licenze a esso associate. Di seguito sono elencate le voci di interfaccia della scheda **Licenze**:

- Nome del prodotto
- Piano di servizio/Versione
- Postazioni utilizzate
- Postazioni fornite
- Data di scadenza
- Stato rinnovo automatico

Stato delle impostazioni di sicurezza

È possibile visualizzare lo stato delle impostazioni di sicurezza in tempo reale facendo clic su **Clienti** > **{nome cliente}** > **{prodotto} nella struttura di rete** > **{gruppo}** > **Impostazioni di sicurezza (riquadro a destra)**.

FIGURA 3-4. Stato delle impostazioni di sicurezza in tempo reale

È possibile visualizzare entrambe le impostazioni In ufficio e Fuori ufficio (solo in Worry-Free Business Security Standard e Advanced). Per controllare le impostazioni, servirsi del menu a discesa Impostazioni. Le impostazioni Fuori ufficio saranno valide soltanto dopo l'attivazione di Location Awareness.

Per ulteriori informazioni, consultare *Barra dei menu a pagina 3-26* e *Comandi di Worry-Free Business Security a pagina 3-27*.

Location Awareness

Utilizzando Location Awareness (solo in Worry-Free Business Security Standard e Advanced), gli amministratori possono controllare le impostazioni di sicurezza in base

alla modalità di collegamento del client alla rete. Worry-Free Business Security Standard e Advanced identifica automaticamente la posizione del client e controlla i siti Web a cui possono accedere gli utenti. Le limitazioni differiscono in base alla posizione dell'utente. Worry-Free Business Security classifica i client in:

- **Client normali**: i computer client fissi con una connessione di rete costante al Security Server.
- **Client roaming**: i client roaming sono computer che non mantengono sempre una connessione di rete costante a Security Server, come ad esempio i computer portatili. I Client/Server Security Agent di questi client continuano a fornire una protezione antivirus, ma si verificano dei ritardi nell'invio a Security Server delle informazioni sullo stato.

Nota

Location Awareness controlla le impostazioni di connessione In ufficio/Fuori ufficio.

Barra dei menu

La barra dei menu nel riquadro a destra viene visualizzata solo quando nella struttura di rete è selezionato Worry-Free o Hosted Email Security. Questi comandi consentono di gestire aspetti critici della sicurezza della rete, tra cui le impostazioni di scansione in tempo reale e l'implementazione degli aggiornamenti dei componenti. Per un elenco dei comandi di rete nella barra dei menu e per istruzioni sul relativo utilizzo, vedere *Comandi di Worry-Free Business Security a pagina 3-27*.

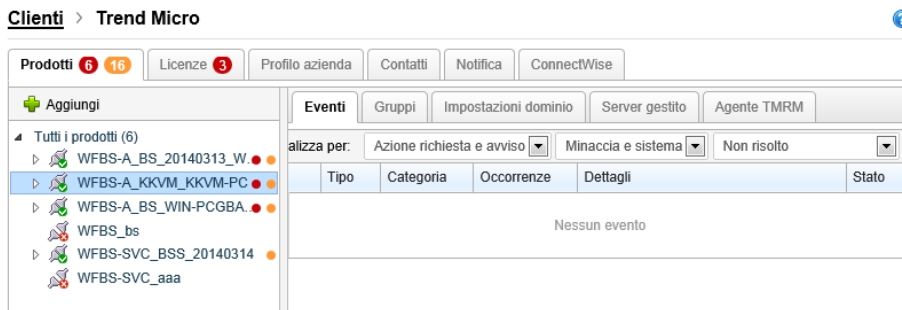



FIGURA 3-5. Barra dei menu

Nota

Le voci sulla barra dei menu sono disattivate e non rispondono ai clic del mouse se l'oggetto di rete selezionato non può ricevere comandi.

Endpoint

Se si seleziona un computer desktop o un server nella struttura di rete, Trend Micro Remote Manager mostra le informazioni relative all'endpoint in questione. Le informazioni visualizzate variano a seconda che l'endpoint sia un server/desktop o un server Exchange. Per visualizzare queste informazioni, visitare la pagina **Clienti** > **{nome cliente}** > **{prodotto}** > **{gruppo}** > **Dispositivi (riquadro a destra)**. Remote Manager™ mostra le seguenti informazioni:

FIGURA 3-6. Stato dell'endpoint

- Nome
- Indirizzo IP
- Stato
- Motore antivirus
- Pattern antivirus
- Versione piattaforma

Comandi di Worry-Free Business Security

I comandi di Worry-Free Business Security (Standard e Advanced) consentono di gestire gli aspetti critici della sicurezza, come l'implementazione dei componenti di sicurezza,

l'analisi dei computer alla ricerca di virus e vulnerabilità note e l'aggiornamento dei server gestiti.

Nota

I comandi di questa sezione sono disponibili solo per Worry-Free Business Security (Standard e Advanced). Per Worry-Free Business Security Services e Hosted Email Security, è necessario accedere alle rispettive console Web.

Nella tabella riportata di seguito sono elencati i comandi del menu Impostazioni di Worry-Free Business Security (Standard e Advanced).

TABELLA 3-2. Comandi del menu Impostazioni

COMANDO	OPERAZIONE	EFFETTI
Scansione manuale	Consente di avviare o interrompere una scansione di un intero dominio.	Consente la scansione manuale su richiesta.
Aggiorna ora	Consente di implementare i componenti per la sicurezza più recenti, tra cui il motore di scansione e i file di pattern.	Consente aggiornare componenti su richiesta.
Antivirus/Anti-spyware in tempo reale	Consente di attivare/disattivare gli scanner antivirus/anti-spyware in tempo reale su tutti i computer del dominio.	La scansione in tempo reale comporta la scansione automatica dei file a cui si accede. La disattivazione della scansione in tempo reale pone in pericolo il dominio.
Scansione in tempo reale per la posta POP3	Attivare/disattivare la scansione in tempo reale per la posta POP3 di tutto il dominio.	POP3 Mail Scan (attraverso il plug-in nella barra degli strumenti di Trend Micro Anti-Spam) protegge i computer dai rischi alla sicurezza e dallo spam trasmesso attraverso i messaggi e-mail POP3.

COMANDO	OPERAZIONE	EFFETTI
Consente il monitoraggio del comportamento	Attivare/disattivare il monitoraggio del comportamento per tutto il dominio.	Il monitoraggio del comportamento protegge i computer da modifiche non autorizzate al sistema operativo, alle voci di registro, ad altri programmi, file e cartelle.
Location Awareness	Consente di attivare/ disattivare Location Awareness per tutto il dominio.	Location Awareness consente agli amministratori di controllare le impostazioni di sicurezza in base a come il client si collega alla rete. Queste impostazioni incidono sulle impostazioni In ufficio/Fuori ufficio di Firewall, Web Reputation e delle barre degli strumenti TrendSecure: funzioni anti-keylogger, crittografia uso dei tasti, classificazione pagine. Se la funzione Location Awareness è disattivata, le impostazioni predefinite sono le impostazioni In ufficio. Le impostazioni Fuori ufficio sono disponibili solo se la funzione Location Awareness è attivata.
Firewall	Consente di attivare/ disattivare il firewall personale per tutto il dominio.	In base alle regole del firewall esistenti, l'abilitazione del firewall può limitare la capacità dei computer di comunicare con la rete. La disattivazione può esporre i computer a un traffico di rete indesiderato.
Reputazione Web	Consente di configurare Web Reputation per tutto il dominio.	Web Reputation impedisce l'accesso agli URL che costituiscono rischi potenziali per la sicurezza controllando tutti gli URL digitati nel database sulla sicurezza Web di Trend Micro.

COMANDO	OPERAZIONE	EFFETTI
Filtri URL	Attiva/Disattiva i filtri URL per tutto il dominio.	Se si attivano i filtri URL, vengono monitorati i tentativi di accesso a siti Web non autorizzati. Questa operazione è disponibile solo per Worry-Free Business Security Services e Worry-Free Business Security Advanced 6.0 versioni successive.
Controllo dispositivi	Attivare/disattivare il controllo dei dispositivi per tutto il dominio.	Se si attiva il controllo dei dispositivi, vengono monitorati i tentativi non autorizzati di accesso a dispositivi. Questa operazione è disponibile solo per Worry-Free Business Security Advanced 7.x e 8.0.
Avvia valutazione delle vulnerabilità	Consente di avviare la valutazione delle vulnerabilità (VA) per la scansione dei computer nel dominio alla ricerca di vulnerabilità note.	Consuma alcune risorse sui computer e aumenta leggermente il traffico tra il server gestito e i computer.
Avvia Damage Cleanup Service	Consente di implementare Damage Cleanup Services (DCS) per la disinfezione dei computer infetti.	Consuma alcune risorse sui computer e può aumentare leggermente il traffico tra il server gestito e i computer.
Aggiorna server gestito	Consente di implementare i più recenti componenti per la sicurezza, tra cui il motore di scansione e i file di pattern, solo sul server gestito.	Verificare che sui computer siano in esecuzione i componenti di protezione aggiornati. L'implementazione può aumentare il traffico tra i computer e il server gestito.

Comando	Operazione	Effetti
Aggiorna Client/ Server Security Agent	Consente di implementare i più recenti componenti per la sicurezza, tra cui il motore di scansione e i file di pattern, su tutti gli Agent Client/Server Security (CSA) nel dominio.	Verificare che sui computer siano in esecuzione i componenti di protezione aggiornati. L'implementazione può aumentare il traffico tra i computer e il server gestito.

Aggiornamento di dati e impostazioni di Hosted Email Security

Per visualizzare le impostazioni e i dati di Hosted Email Security, tra i quali Stato in tempo reale, Impostazioni globali e Informazioni su, fare clic sulla scheda **Clienti** > **{cliente}** > **Hosted Email Security**.

Le informazioni seguenti sono mostrate per tutti i domini e vengono aggiornate una volta al giorno:

- Tutte le informazioni nella scheda **Stato in tempo reale**.
- **Impostazioni dei criteri**
- **Mittenti approvati**
- Tutte le informazioni nella scheda **Informazioni licenza**.

Nota

L'aggiornamento dei nuovi dati di Hosted Email Security sulla console Web Remote Manager può richiedere un massimo di tre ore.

Notifiche

È possibile inviare le notifiche ai clienti sotto forma di messaggi e-mail oppure è possibile visualizzarle nel widget **Notifiche** o nel software di terzi.

Viene visualizzata la schermata **Configura notifiche**. In questa pagina è possibile impostare:

- Eventi che attivano notifiche:
    - Eventi correlati alla licenza:
        - **In scadenza**: se vi sono licenze prossime alla scadenza, viene inviata una notifica. È inoltre possibile impostare la frequenza con la quale il sistema invia una notifica.
            - **Frequenza mensile**: il sistema invia una notifica e-mail ogni 30 giorni, a partire da 60 giorni prima della scadenza.
            - **Frequenza quattordicinale**: il sistema invia una notifica e-mail ogni 14 giorni, a partire da 28 giorni prima della scadenza.
            - **Frequenza settimanale**: il sistema invia una notifica e-mail ogni 7 giorni, a partire da 14 giorni prima della scadenza.

Nota

Anche se si è impostata la notifica per l'invio di un messaggio e-mail solo con frequenza settimanale, quattordicinale o mensile, è possibile ricevere una notifica e-mail ogni giorno poiché quest'ultima dipende dalla data di scadenza relativa a un'azienda. Tuttavia, per evitare di ricevere diverse notifiche e-mail nello stesso giorno, Trend Micro include nel medesimo messaggio anche i nomi dell'azienda e le date di altri prodotti prossimi alla scadenza.

- **Scaduto**: viene inviata una notifica se vi sono licenze scadute.
- **Allocazione in eccesso**: viene inviata una notifica se la percentuale di postazioni utilizzate supera il numero di quelle fornite. È possibile specificare la percentuale di postazioni utilizzate che hanno superato quelle fornite al cliente. Tale percentuale può essere un valore compreso tra 100 e 120.

- Eventi correlati al prodotto:
    - Eventi Worry-Free Business Security e Worry-Free Business Security Services:
        - **Minacce**: viene inviata una notifica se il numero di eventi di minaccia supera la soglia specificata.

- **Sistema**: viene inviata una notifica se il numero di eventi di sistema o dispositivo supera la soglia specificata.

  - Eventi Cloud Edge:

    - **Eccedenze minacce Web rilevate**: viene inviata una notifica se il numero di minacce Web rilevate supera la soglia specificata.

- Destinatari della notifica:

  - **Kaseya** (solo eventi Worry-Free Business Security e Worry-Free Business Security Services)

  - **Autotask** (solo eventi Worry-Free Business Security e Worry-Free Business Security Services)

  - **ConnectWise**

  - **Io**: indirizzo e-mail che riceve la notifica e-mail.

Nota

Se l'indirizzo e-mail non è corretto, fare clic sul collegamento **Licensing Management Platform** o sul pulsante **Account** per accedere alla pagina di configurazione del profilo e modificarne le impostazioni.

  - **Ulteriori destinatari**: è possibile specificare ulteriori destinatari del messaggio e-mail per eventi specifici del cliente.

Per ulteriori informazioni e su come configurare la notifica, fare riferimento a *Configurazione delle notifiche a pagina 8-2*.

Aggiornamenti dei dati e dello stato di Worry-Free Business Security Services

Per visualizzare le impostazioni e i dati di Worry-Free Business Security Services, incluso lo stato, fare clic su **Clienti** > **{nome cliente}** > **{prodotto}** > **WFBS-SVC**.

Le informazioni di Worry-Free Business Security Services vengono aggiornate una volta al giorno. Queste comprendono:

- Tutte le informazioni in **Impostazioni di sicurezza**.

- La **Data di scadenza** nella scheda **Informazioni licenza** (è la data di scadenza del codice di attivazione di Worry-Free Business Security Services).

Nota

L'aggiornamento dei nuovi dati di Worry-Free Business Security Services sulla console Web Remote Manager può richiedere un massimo di tre ore.

le opzioni visualizzate possono variare in base al meccanismo di licenza utilizzato.

Capitolo 4

Preparazione dell'infrastruttura

In questa sezione sono trattati i seguenti argomenti:

Panoramica sull'installazione dell'infrastruttura

In genere, la preparazione dell'infrastruttura dei servizi implica, per ciascun tipo di prodotto/servizio, le seguenti operazioni.

Worry-Free Business Security Standard e Advanced

1. Aggiunta di un nuovo cliente alla console Web Remote Manager.
2. Aggiunta del contatto cliente principale.
3. Aggiunta di almeno un prodotto al cliente.
4. Installazione dell'Agent sul server del cliente.
5. Inserimento del GUID o della chiave di autorizzazione nell'Agent.

Hosted Email Security e Worry-Free Business Security Services

1. Aggiunta di un nuovo cliente alla console Web Remote Manager.
2. Aggiunta del contatto cliente principale.
3. Aggiunta di almeno un servizio al cliente.
4. Immissione della chiave di autorizzazione nella console dei servizi del cliente.

ConnectWise

1. Collegamento di Connectwise e aggiunta delle relative credenziali di accesso su **Amministrazione** > **Configura integrazione di terzi (schermata)** sulla console Web Remote Manager.
2. Definizione delle impostazioni di notifica ConnectWise globali.
3. Aggiunta del destinatario delle notifiche all'elenco dei destinatari in **Clienti** > **{cliente}** > **Notifica (scheda)** sulla console Web Remote Manager.

4. Aggiunta dei campi necessari alla console ConnectWise.
5. Configurazione delle impostazioni ConnectWise e della notifica per ciascun cliente (opzionale).

Kaseya

1. Collegamento di Kaseya e aggiunta dell'indirizzo e-mail dell'utente Kaseya su **Amministrazione** > **Configura integrazione di terzi (schermata)** sulla console Web Remote Manager.
2. Aggiunta del destinatario delle notifiche all'elenco dei destinatari in **Clienti** > **{cliente}** > **Notifica (scheda)** sulla console Web Remote Manager.
3. Aggiunta dei campi necessari alla console Kaseya.

Autotask

1. Collegamento di Autotask e aggiunta delle relative credenziali di accesso su **Amministrazione** > **Configura integrazione di terzi (schermata)** sulla console Web Remote Manager.
2. Aggiunta del destinatario delle notifiche all'elenco dei destinatari in **Clienti** > **{cliente}** > **Notifica (scheda)** sulla console Web Remote Manager.
3. Aggiunta dei campi necessari alla console Autotask.

Aggiunta di prodotti

Aggiunta di clienti

È necessario identificare le informazioni di base sul cliente prima di crearne l'account. Le informazioni richieste includono **Nome e cognome** (come verranno inseriti in rapporti e notifiche), **Fuso orario** (del cliente) e **Lingua** (in cui redigere rapporti e notifiche). Prima di aggiungere un cliente e installare l'Agent sul server gestito, assicurarsi di avere

l'approvazione scritta per eseguire le operazioni di accesso, monitoraggio e gestione delle risorse del cliente.

Procedura

1. Nel banner della console Web Remote Manager, fare clic su **Nuovo cliente**.

Nota

È possibile fare clic su **Nuovo cliente** dal banner o dalla scheda **Clienti**.

2. Fornire le informazioni sul cliente.

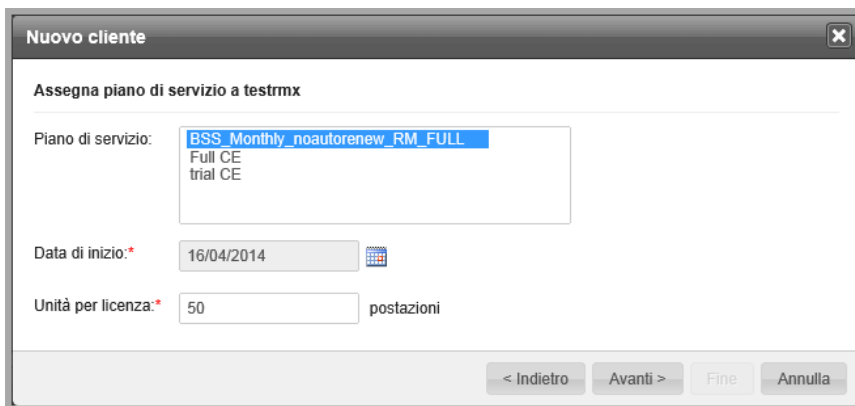



Figura 4-1. Schermata Info cliente

3. Fare clic su **Avanti >**.

4. Assegnare un piano di servizio, una data di inizio e il numero di unità per licenza.

5. Configurare le impostazioni predefinite del prodotto per l'account specificato. Tali impostazioni sono:

Nota

Questa funzione è disponibile sono per Worry-Free Business Security Services.

- **Impostazioni prodotto di base**: configurare solo le impostazioni nella schermata che vengono utilizzate dai nuovi account cliente.

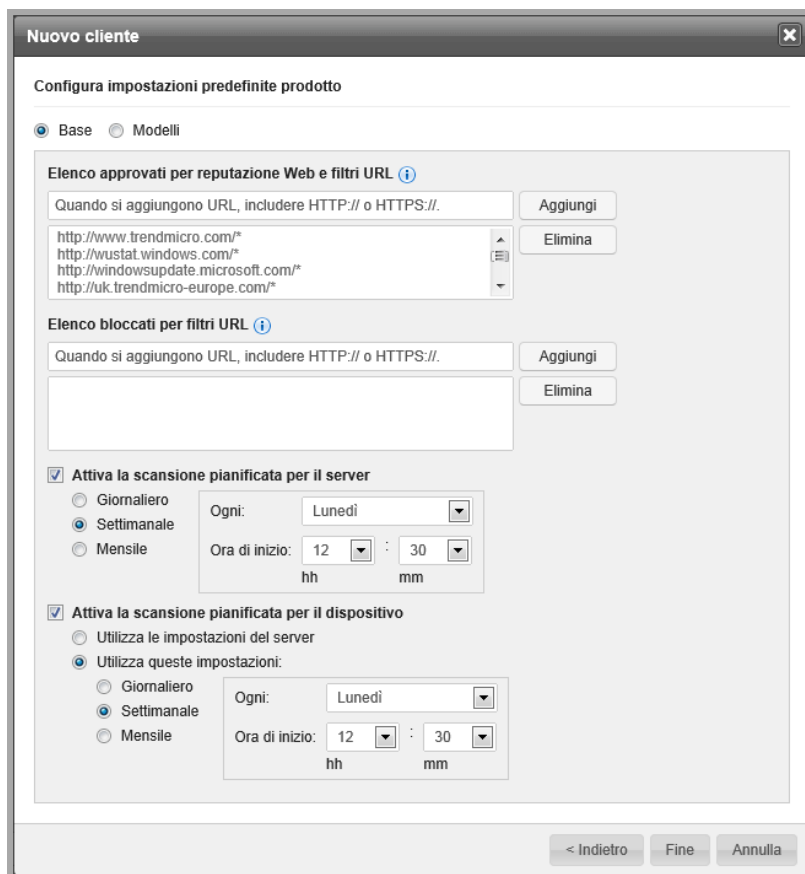



FIGURA 4-2. Impostazioni prodotto di base

- **Modelli**: utilizzare questa opzione per selezionare un modello di impostazione predefinita. Configurare le impostazioni in **Amministrazione** > **Configura modelli impostazione predefinita**.

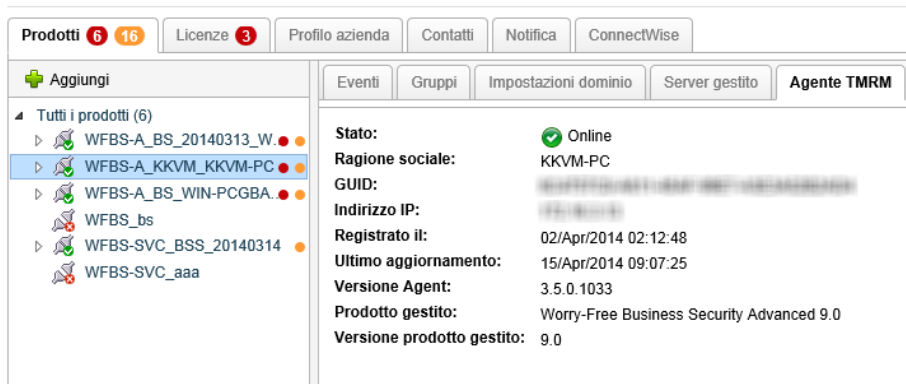
6. Verificare tutte le informazioni, quindi fare clic su **Fine**.

Nota

Dopo aver aggiunto il cliente, è possibile modificare il profilo solo da Trend Micro Licensing Management Platform.

Registrazione dei prodotti Trend Micro in Trend Micro Remote Manager

È possibile registrare prodotti Trend Micro in Trend Micro Remote Manager. Per i prodotti di terzi, fare riferimento a *Integrazione di prodotti di terzi con Trend Micro Remote Manager a pagina 4-16*.

Registrazione di Worry-Free Business Security

In questa sezione sono fornite informazioni utili per comprendere come connettere o disconnettere Worry-Free Business Security da Trend Micro Remote Manager.

GUID dell'Agent o chiave di autorizzazione

Per distinguere tra prodotti e servizi, Remote Manager assegna un GUID (Globally Unique Identifier) o una chiave di autorizzazione a ciascuno di essi. Ogni volta che si aggiunge un prodotto o un servizio alla console Web Remote Manager, Remote Manager genera un nuovo GUID o una nuova chiave di autorizzazione. La persona che installa l'Agent sul server gestito o aggiunge un servizio alla console Web Remote Manager deve immettere il GUID o la chiave di autorizzazione durante l'installazione per consentire la registrazione del prodotto in Remote Manager.

I GUID o le chiavi di autorizzazione per i prodotti e i servizi di un cliente sono sempre disponibili in: **Clienti** > **Tutti i clienti (nella struttura)** > **{cliente}** > **Agente TMRM (scheda)**.

FIGURA 4-3. I GUID dell'Agent o le chiavi di autorizzazione sono sempre disponibili (Worry-Free Business Security Standard e Advanced)

GUID dell'Agent Remote Manager

```
1A2B3C4567D8-E1FGHI23-J456-78K9-1L23
```

Installazione dell'Agent per Worry-Free Business Security 6,0 e versioni successive

Esistono vari modi per installare l'Agent Trend Micro Remote Manager in Worry-Free Business Security Standard o Advanced 6.0 e versioni successive. Le procedure di installazione variano a seconda che il cliente sia nuovo o disponga già di un account esistente sulla console Web Remote Manager.

Informazioni preliminari

- GUID dell'Agent Remote Manager
- Programma di installazione dell'Agent (`WFRMAgentforWFBS.exe`)

- Connessione Internet attiva
- 50 MB di spazio disponibile sul disco rigido

Clienti senza account Remote Manager

Procedura

- Opzione 1: Dalla console Web Remote Manager
    1. Dalla console Web Remote Manager, aggiungere il cliente e fornire una descrizione facoltativa.
    2. Aggiungere Worry-Free Business Security Standard o Advanced alla console Web Remote Manager, la quale genera un GUID nella procedura.
    3. Installare l'Agent Remote Manager sul server Worry-Free Business Security Standard o Advanced utilizzando il GUID generato dalla console.
- Opzione 2: Installare l'Agent sul server Worry-Free Business Security

    Per installare l'Agent, utilizzare il programma di installazione dell'Agent Remote Manager sul server Worry-Free Business Security (non aggiungere prima il cliente alla console Web Remote Manager).

Clienti con account Remote Manager

Procedura

1. Aggiungere Worry-Free Business Security Standard o Advanced alla console Web Remote Manager, la quale genera un GUID nella procedura.
2. Installare l'Agent Remote Manager sul server Worry-Free Business Security Standard o Advanced utilizzando il GUID generato dalla console.

Verifica dell'installazione dell'Agent Trend Micro Remote Manager

Verificare che l'Agent sia stato installato correttamente.

Verifica dello stato del servizio dell'Agent

Sul computer in cui è installato l'Agent Remote Manager, verificare se `Trend Micro Information Center for CSM` è stato avviato.

Procedura

1. Fare clic su **Start** > **Impostazioni** > **Pannello di controllo** > **Strumenti amministrativi** > **Servizi**.
2. Cercare **Trend Micro Remote Manager Agent**.
3. Verificare che per **Stato** sia indicato **Avviato**.

Verifica dei collegamenti del menu Start

Sul computer in cui è installato l'Agent Trend Micro Remote Manager, verificare la presenza del gruppo di programmi nel menu Start.

Procedura

1. Fare clic su **Start** > **Programmi** > **Trend Micro Remote Manager Agent**.
2. Verificare che il gruppo di programmi contenga gli elementi elencati di seguito:
   - Agent Configuration Tool
   - Readme

Verifica dell'icona sulla barra delle applicazioni

Sulla barra delle applicazioni del computer in cui è installato l'Agent Trend Micro Remote Manager, verificare la presenza dell'icona dell'Agent Trend Micro Remote Manager. Se per qualche motivo l'icona non è visibile, avviare l'Agent facendo clic su

Start > **Programmi** > **Trend Micro Remote Manager Agent** > **Agent Configuration Tool**.

L'uscita dallo strumento non provoca l'arresto del servizio Trend Micro Remote Manager, ma semplicemente la chiusura di Agent Configuration Tool e la rimozione dell'icona dalla barra delle applicazioni. Lo strumento può essere riavviato in qualsiasi momento.

Posizionare il puntatore del mouse sull'icona per visualizzare le informazioni sullo stato.

TABELLA 4-1. Icone sulla barra delle applicazioni

ICONA	DESCRIZIONE
	Un'icona verde indica che l'Agent è connesso al server di comunicazione di Trend Micro Remote Manager. L'Agent funziona normalmente.
	Un'icona rossa indica che l'Agent non è connesso al server di comunicazione di Trend Micro Remote Manager o che la versione dell'Agent non corrisponde al server ed è necessario aggiornarla.
	Un'icona con una freccia rossa indica che l'Agent è stato disconnesso da Trend Micro Remote Manager.
	Un'icona con una X rossa indica che l'Agent è stato disconnesso.

Controllo della connessione tra Agent e server

Per garantire che il servizio Trend Micro Remote Manager sia in esecuzione senza problemi, verificare che lo stato degli Agent visualizzato nella console Remote Manager sia "connesso" o "online".

Accedere a **Clienti** > **{cliente}** > **Prodotti (scheda)**.

Nella colonna **Stato** della struttura è indicato lo stato di ciascun Agent. Per informazioni su ogni stato, vedere *Stato dell'Agent a pagina 6-2*.

Oltre alla sezione corrente, fare riferimento a *Risoluzione dei problemi e problemi noti a pagina 11-1* per ulteriori problemi relativi alla connettività server/Agent.

Visualizzazione degli errori di installazione

I registri di installazione dell'Agent registrano le attività di installazione dell'Agent. Questi registri possono essere raccolti e inviati al fornitore del supporto qualora si riscontrino problemi durante l'installazione. È possibile ottenere i registri di installazione dell'Agent dal seguente percorso sul server gestito:

```
C:\WFRMAgentForCSM_Install.log
```

Registrazione di Worry-Free Business Security Services

In questa sezione sono fornite informazioni su come connettere o disconnettere Worry-Free Business Security Services da Trend Micro Remote Manager.

Connessione di un cliente Worry-Free Business Security Services alla console Web Remote Manager

Per gestire Worry-Free Business Security Services dalla console Web Trend Micro Remote Manager, è necessario registrare un account Worry-Free Business Security Services con Remote Manager eseguendo le operazioni seguenti:

Nota

Se il rivenditore ha aggiunto il prodotto all'account da Licensing Management Platform, non è necessario seguire i passaggi successivi.

Procedura

1. Aggiungere il prodotto alla console Web Remote Manager e salvare il GUID o la chiave di autorizzazione.

   Per ulteriori informazioni, fare riferimento a *Aggiunta di prodotti/servizi a pagina 5-8*.

2. Accedere all'account Worry-Free Business Security Services del cliente.

3. Accedere a **Amministrazione** > **Trend Micro Remote Manager**.

4. Digitare la chiave di autorizzazione e fare clic su **Connetti**.

Disconnessione di un cliente Worry-Free Business Security Services dalla console Web Remote Manager

Per disconnettere un cliente Worry-Free Business Security Services dalla console Web Remote Manager, procedere come segue:

- Se l'account è stato integrato con Licensing Management Platform, il rivenditore può eliminare il piano di servizio dalla console Web Licensing Management Platform. Dopo aver eliminato il piano di servizio, il cliente viene disconnesso dalla console Web Remote Manager.
- Per gli altri account, il cliente può aprire la schermata di Remote Manager nella console Web Worry-Free Business Security Services e fare clic su **Scollega**.

Il cliente riceverà quindi una notifica sulla console Worry-Free Business Security Services.

Registrazione di Hosted Email Security

In questa sezione sono fornite informazioni su come connettere o disconnettere Hosted Email Security da Trend Micro Remote Manager.

Connessione di un cliente Hosted Email Security alla console Web Remote Manager

Per poter gestire Hosted Email Security dalla console Web Trend Micro Remote Manager, è necessario registrare un account Hosted Email Security per il cliente in Remote Manager.

Nota

Se il rivenditore ha aggiunto il prodotto all'account da Licensing Management Platform, non è necessario seguire i passaggi successivi.

Procedura

1. Aggiungere il prodotto alla console Web Remote Manager e salvare il GUID o la chiave di autorizzazione.

2. Accedere all'account Hosted Email Security del cliente.

3. Accedere a **Amministrazione** > **Remote Manager**.

4. Digitare il GUID o la chiave di autorizzazione e fare clic su **Connetti**.

    Dopo aver inserito il GUID o la chiave di autorizzazione e aver fatto clic su **Connetti**, possono essere necessari anche 10 minuti prima che Hosted Email Security completi il collegamento alla console Web Remote Manager.

5. Esaminare lo stato della connessione.

    L'aggiornamento dei nuovi dati di Hosted Email Security sulla console Web Remote Manager può richiedere un massimo di tre ore. Le informazioni sui clienti Hosted Email Security vengono aggiornate una volta al giorno. Vedere *Aggiornamento di dati e impostazioni di Hosted Email Security a pagina 3-31*.

Disconnessione di un cliente Hosted Email Security dalla console Web Remote Manager

Per disconnettere un cliente Hosted Email Security dalla console Web Remote Manager, procedere come segue:

- Se l'account è stato integrato con Licensing Management Platform, il rivenditore può eliminare il piano di servizio dalla console Web Licensing Management Platform. Dopo aver eliminato il piano di servizio, il cliente viene disconnesso dalla console Web Remote Manager.

- Per gli altri account, il cliente può aprire la schermata di Remote Manager nella console Web Hosted Email Security e fare clic su **Interrompi**.

Il cliente riceve quindi una notifica sulla console Hosted Email Security e deve fare clic su **OK**.

Integrazione di prodotti di terzi con Trend Micro Remote Manager

È possibile registrare prodotti di terzi in Trend Micro Remote Manager. Per i prodotti Trend Micro, fare riferimento a *Registrazione dei prodotti Trend Micro in Trend Micro Remote Manager a pagina 4-8*.

Integrazione di Autotask™

Configurare le seguenti impostazioni per integrare Autotask™ con Remote Manager:

Configurazione delle impostazioni Autotask in Remote Manager

Procedura

1. Fare clic su **Amministrazione** > **Configura integrazione di terzi**.

   Viene visualizzata la finestra **Integrazione di terzi**.

   Autotask

   ☐ Attiva integrazione

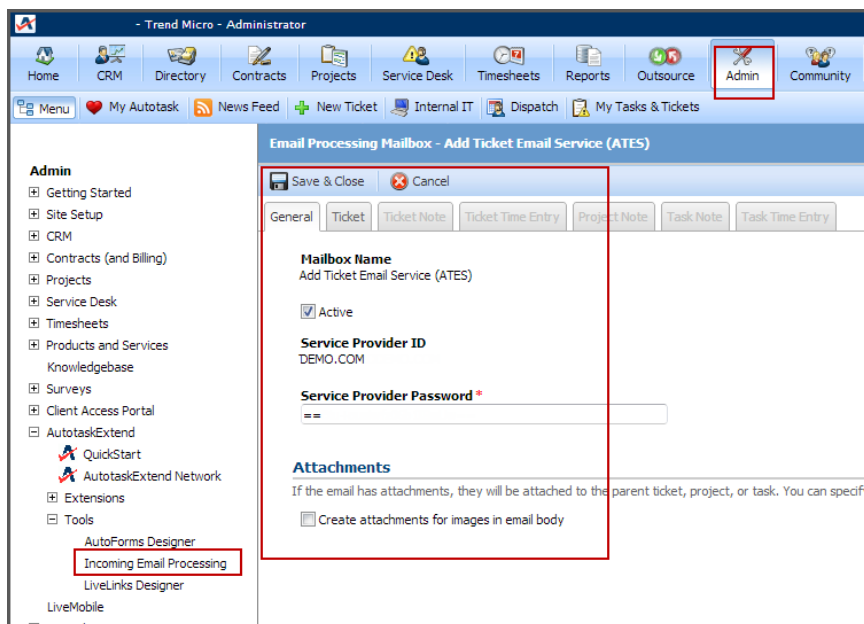
   ID accesso:

   Password di accesso:

   Lingua: Inglese

   FIGURA 4-4. Casella di gruppo Notifiche di Informazioni account

2. Fare clic su **Attiva integrazione**.

3. Specificare le credenziali di accesso. È possibile verificare le credenziali Autotask in **Amministrazione** > **AutotaskExtend** > **Strumenti** > **Elaborazione e-mail in entrata** > **Aggiungi servizio e-mail ticket (ATES)** > **Modifica** > **Impostazioni generali**.

4. Selezionare la lingua preferita.
5. Fare clic su **Salva**.
6. Fare clic su **Clienti** > **Tutti i clienti (nella struttura)** > **{cliente}** > **Notifiche (scheda)**.

Clienti › Trend Micro

Prodotti 6 16 | Licenze 3 | Profilo azienda | Contatti | Notifica | ConnectWise

Eventi

- Utilizza le impostazioni di notifica in tempo reale predefinite
- Utilizza le impostazioni personalizzate

Tutti gli eventi di licenza

Evento	E-mail	Frequenza e-mail	Soglia di avviso
In scadenza	☑	Una volta ogni due settimane	Licenza in scadenza tra 28 giorni
Scaduto	☑	Per evento	
Allocazione in eccesso	☑	Per evento	Eccedenze allocazioni (%): 100

Worry-Free Business Security Services

Evento	E-mail
Minaccia	☑
Sistema	☑

Worry-Free Business Security

Evento	E-mail
Minaccia	☑
Sistema	☑

Cloud Edge

Evento	E-mail	Soglia di avviso
Rilevate minacce Web in eccesso	☑	Eccedenze minacce Web: 1 (1-300)

Destinatari

Nota: Attivare l'integrazione con strumenti di terzi per poter ricevere le notifiche. A tal fine, accedere a Amministrazione > Configura integrazione di terzi. Per ConnectWise, è anche necessario attivare l'impostazione per clienti specifici facendo clic sulla scheda ConnectWise nella pagina del cliente.

- ConnectWise
- Kaseya (solo eventi Worry-Free Business Security e Worry-Free Business Security Services)
- Autotask (solo eventi Worry-Free Business Security e Worry-Free Business Security Services)

Ulteriori destinatari:

Separare più voci con un punto e virgola.

Salva | Annulla

FIGURA 4-5. Selezione delle notifiche richieste

7. Selezionare le notifiche da inviare ad Autotask relative a Worry-Free Business Security Services.

8. Selezionare Autotask tra i destinatari.

9. Ripetere i punti 5, 6 e 7 per ciascun cliente.

Configurazione delle impostazioni in Autotask

Procedura

1. In Autotask, per aggiungere i campi seguenti al sistema di ticketing, accedere a **Amministrazione** > **Service Desk** > **Tipi di problemi e sottoproblemi** > **Avviso servizi gestiti**. In tal modo si attiva la visualizzazione delle notifiche Trend Micro Remote Manager in Autotask. Scegliere tra i seguenti avvisi di servizio gestito:

    - Eventi di minaccia Trend Micro
    - Eventi di sistema Trend Micro
    - Eventi di licenza Trend Micro

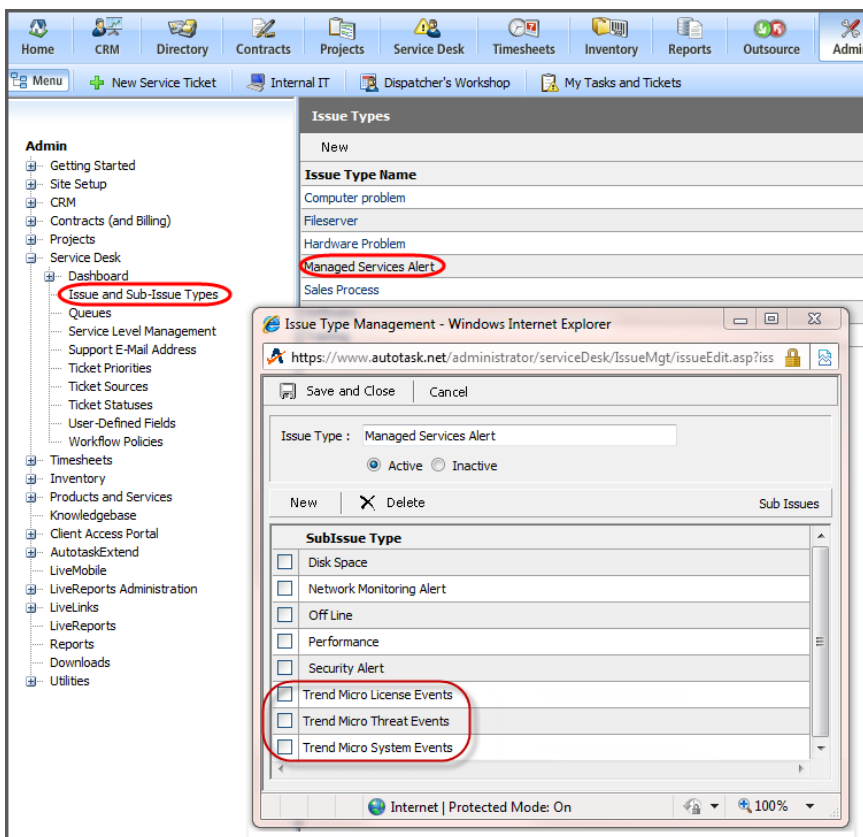



FIGURA 4-6. Tipi di problemi e sottoproblemi Trend Micro

2. Accedere a **Amministrazione** > **AutotaskExtend** > **Strumenti** > **Elaborazione e-mail in entrata** > **Aggiungi servizio e-mail ticket (ATES)** > **Modifica** > **Ticket** e verificare che l'impostazione relativa all'e-mail sia corretta:

3. Accedere a **Amministrazione** > **Configurazione sito** > **Campi definiti dall'utente** e definire il campo Trend Micro ID sito.

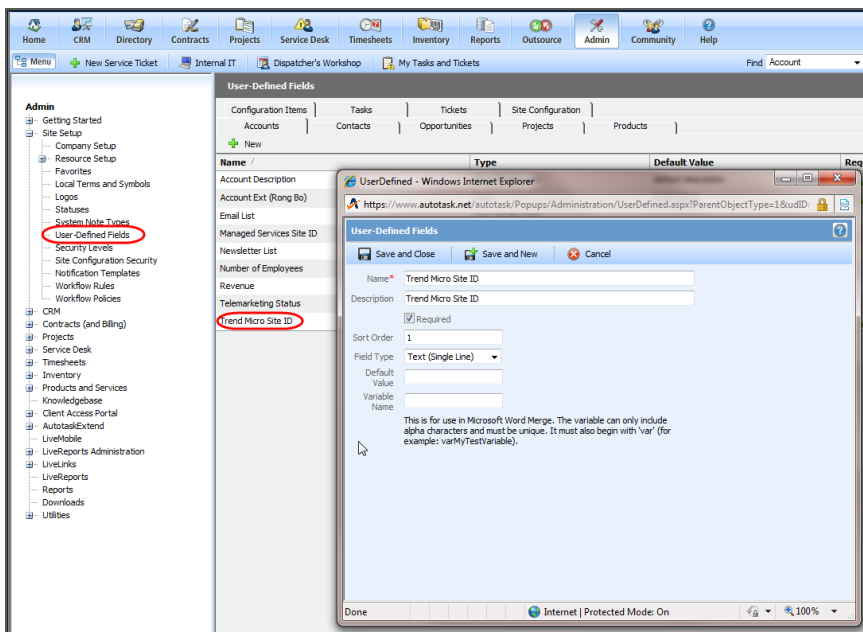
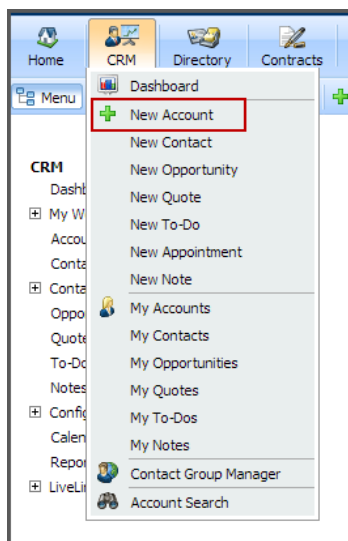



FIGURA 4-7. Definizione del campo Trend Micro ID sito

4. Accedere a **CRM** > **Nuovo account** e immettere l'ID univoco Remote Manager nel nuovo campo Trend Micro ID sito.

   Corrisponde all'ID univoco esportato da Remote Manager.

Integrazione di Kaseya™

Configurare le seguenti impostazioni per integrare Kaseya™ con Remote Manager:

Configurazione delle impostazioni in Remote Manager

Procedura

1. Fare clic su **Amministrazione** > **Configura integrazione di terzi**.

   Viene visualizzata la finestra **Integrazione di terzi**.

Kaseya

☐ Attiva integrazione

Indirizzo e-mail Kaseya:

Figura 4-8. Casella di gruppo Notifiche di Informazioni account

2. Fare clic su **Attiva integrazione**.
3. Aggiungere l'indirizzo e-mail Kaseya.
4. Fare clic su **Salva**.
5. Accedere a **Clienti** > **Tutti i clienti (nella struttura)** > **{cliente}** > **Notifiche (scheda)**.

FIGURA 4-9. Selezione delle notifiche richieste

6. Selezionare le impostazioni di notifica del prodotto da inviare a Kaseya.

Nota

Si devono selezionare le impostazioni predefinite di notifica in tempo reale applicabili a tutti i prodotti e clienti oppure le impostazioni per il cliente specificato.

7. Selezionare Kaseya tra i destinatari.

8. Ripetere i punti 5, 6 e 7 per ciascun cliente.

Configurazione delle impostazioni in Kaseya

Procedura

1. In Kaseya, aggiungere i campi elencati di seguito al sistema di ticketing per visualizzare le notifiche Trend Micro Remote Manager.

   - Worry-Free Business Security

Nome campo	Scopo
TM_CreateTime	Ora di generazione dell'evento
TM_ProductName	Nome del prodotto
TM_AgentGUID	GUID dell'Agent Remote Manager
TM_CustomerName	Nome cliente/azienda
TM_EventName	Nome dell'evento
TM_ServerName	Nome del server Client Server Messaging/Worry-Free Business Security
TM_MASClientName (facoltativo)	Nome del server Exchange (interessa solo l'evento Arresto server Exchange)

FIGURA 4-10. Campi di ticketing di Kaseya

- Worry-Free Business Security Services

NOME CAMPO	SCOPO
TM_CreateTime	Ora di generazione dell'evento
TM_ProductName	Nome del prodotto
TM_CustomerName	Nome cliente/azienda
TM_EventName	Nome dell'evento

FIGURA 4-11. Campi di ticketing di Kaseya

2. Verificare che l'impostazione e-mail sia corretta come illustrato nella seguente schermata:

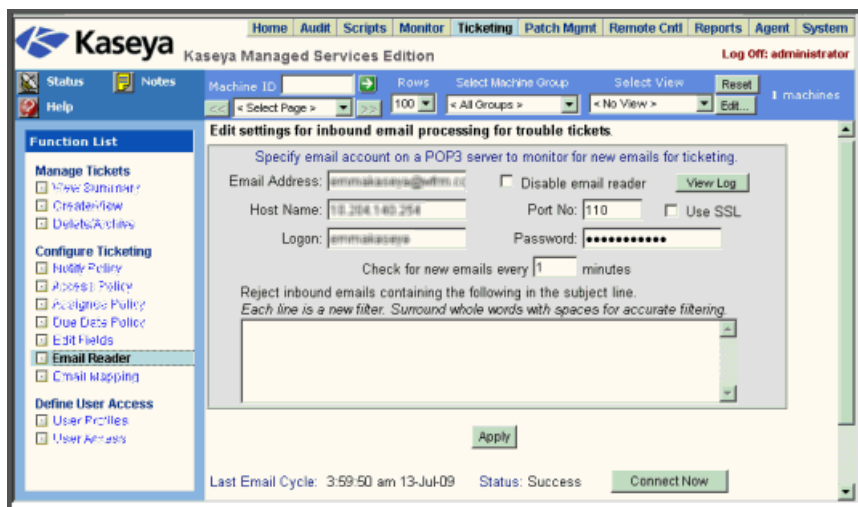



FIGURA 4-12. Impostazioni e-mail di Kaseya

Quando viene attivato un evento, Kaseya riceve il ticket:

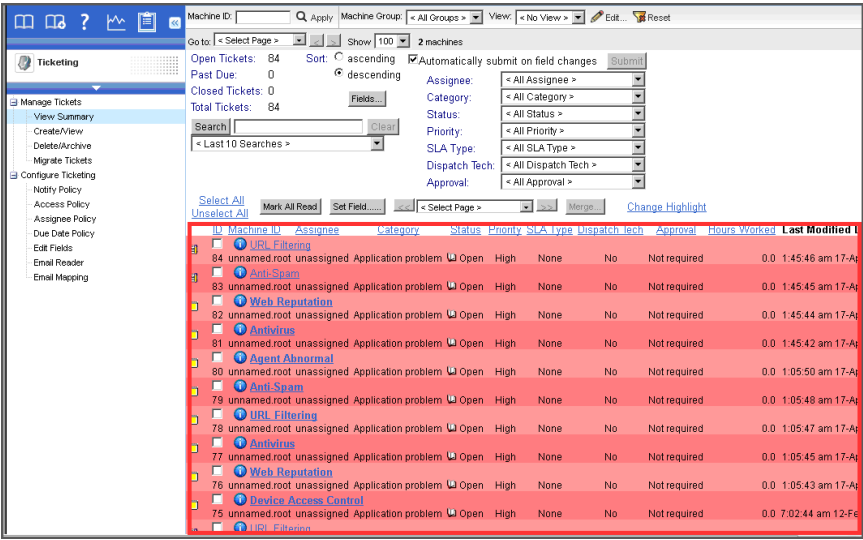



FIGURA 4-13. Ticket evento Kaseya

Integrazione di ConnectWise™

Configurare le seguenti impostazioni per integrare ConnectWise™ con Remote Manager:

Configurazione delle impostazioni generali di ConnectWise in Remote Manager

Procedura

1. Accedere a **Amministrazione** > **Configura integrazione di terzi**.

Viene visualizzata la finestra **Integrazione di terzi**.

ConnectWise

Attiva integrazione

URL ConnectWise: test.connectwise.com

ID azienda: trendmicro

ID accesso: admin1

Password di accesso: ••••••

Test di connessione

Inviare le informazioni sulla fatturazione per tutti i prodotti a ConnectWise ogni mese il 1

Inviare informazioni sul rilevamento di spam/virus da Hosted Email Security a ConnectWise ogni giorno

FIGURA 4-14. Casella di gruppo Notifiche di Informazioni account

2. Modificare i seguenti valori:
    - **Abilita integrazione ConnectWise**: selezionare questa casella di controllo per abilitare l'integrazione tra Trend Micro Remote Manager e ConnectWise.
    - **URL ConnectWise**: inserire l'URL del servizio.
    - **ID azienda**
    - **ID accesso**: l'account utilizzato per accedere a ConnectWise.
    - **Password di accesso**: la password associata all'account.
    - Selezionare la frequenza con cui Remote Manager deve inviare informazioni di fatturazione.
    - Selezionare la frequenza con cui Remote Manager deve inviare le statistiche spam.
3. Fare clic su **Salva**.

Configurazione delle impostazioni di ConnectWise specifiche per i clienti in Remote Manager

Configurazione delle impostazioni di ConnectWise per ciascun cliente. Tali impostazioni sono facoltative. Se tuttavia si desidera ricevere anche una notifica specifica per i clienti, è necessario attivare questa funzione.

Procedura

1. Accedere a **Clienti (scheda)** > **{cliente}** > **ConnectWise (scheda, riquadro a destra)**.

2. Selezionare **Attiva integrazione**.

3. Specificare un **ID azienda** valido presente in ConnectWise.

Nota

Se non si è sicuri dell'ortografia, è possibile fare clic su **Validità test** per verificare l'ID azienda.

4. Selezionare le impostazioni di integrazione.

   - Utilizzare le impostazioni predefinite disponibili in **Amministrazione**.
   - Specificare le opzioni personali per la fatturazione e i riepiloghi esecutivi.

5. Fare clic su **Salva**.

6. Accedere a **Clienti (scheda)** > **{cliente}** > **Notifica (scheda, riquadro a destra)**.

7. Configurazione delle impostazioni di notifica per il cliente specificato.

8. Selezionare **ConnectWise** tra i destinatari.

9. Fare clic su **Salva**.

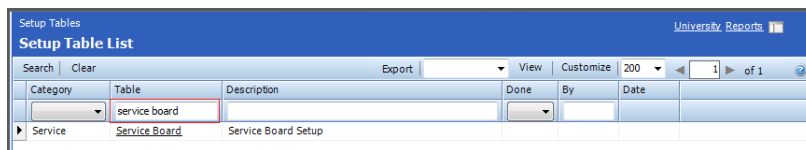
Configurazione delle impostazioni in ConnectWise

Procedura

1. Accedere a ConnectWise mediante lo strumento di automazione dei servizi professionali (PSA).

2. Creare una nuova area servizi.

   Questa operazione è facoltativa, ma è utile perché consente di filtrare efficacemente i risultati di Trend Micro Remote Manager.

   a. Accedere a **Setup** > **Setup Table** > **Search** e digitare `Service Board`.

   b. Fare clic su **Service Board**.

   Viene visualizzato un elenco di aree servizi.

   c. Fare clic sulla nuova icona per creare una nuova area servizi.

Viene visualizzata la schermata della nuova area servizi.

d. Modificare i campi **Board Name**, **Location**, **Business Unit** e **Sign Off Template**. Tutti gli altri campi sono facoltativi.

e. Fare clic su **Salva**.

f. Fare clic sulla scheda **Statuses**.

g. Fare clic sulla nuova icona per creare un nuovo servizio per lo stato.

h. Modificare i campi **Status to Description**, **Sort Order** e selezionare **Display on Board**.

i. Fare clic su **Salva**.

3. Assegnare i privilegi all'utente.

a. Accedere a **Setup** > **Setup Table** > **Search** e digitare `Integrator Login`.

b. Fare clic sul collegamento **Integrator Login** richiesto e quindi sulla nuova icona per creare un nuovo account di accesso.

   Viene visualizzata la schermata **General**.

c. Da **Access Levels**, selezionare **All records**.

d. Selezionare le opzioni seguenti: **Service Ticket API**, **Management Services API**, **Company API**, **System API** e **Configuration API**.

e. Selezionare l'area servizi creata in precedenza, modificare **Ticket Callback URL** in `www.example.com` o in qualsiasi altro URL arbitrario e fare clic su **Salva**.

f. Fare clic su **Salva**.

4. Creare una nuova soluzione di gestione.

a. Accedere a **Setup** > **Setup Table** > **Search** e digitare `Management IT`.

b. Fare clic su **Management IT**.

c. Fare clic sulla nuova icona per creare una soluzione di gestione.

d. Modificare il campo **Name** in `TMRM Management Setup`, **Management IT Solution** in `Custom` e **Custom Solution Name** in `TMRM Management Solution`.

   L'uso di altri valori potrebbe interrompere la connessione.

e. Fare clic su **Salva**.

5. Modificare lo stato predefinito dell'azienda in `Active`.

a. Accedere a **Setup** > **Setup Table** > **Search** e digitare `Company Status`.

b. Fare clic su **Company Status**.

c. Fare clic su **Active**.

d. Selezionare **Default Flag**.

e. Fare clic su **Salva**.

6. Creare un nuovo servizio per ciascun prodotto/servizio Remote Manager gestito.

a. Accedere a **Setup** > **Products** > **New**

b. Sostituire l'**ID del prodotto** con un prodotto/servizio gestito. Scegliere da `HES/WFBS-SVC/WFBS-S/WFBS-A`.

c. Modificare i prezzi in base alle necessità.

d. Fare clic su **Salva**.

Ripetere queste operazioni per ciascun prodotto/servizio gestito.

7. Creare dei riferimenti incrociati per ciascun prodotto/servizio Remote Manager gestito.

a. Accedere a **Setup** > **Setup Table** > **Search** e digitare `Managed Devices Integration`.

b. Fare clic su **Managed Devices Integration**.

c. Selezionare la Management Solution denominata "**Remote Manager Management Solution**".

d. Selezionare la scheda **Cross Reference** > **New**.

e. Modificare i campi in base alle necessità.

Impostazioni per i prodotti/servizi Remote Manager gestiti.

PRODOTTO/SERVIZIO	IMPOSTAZIONI
Worry-Free Business Security Standard	• **Tipo**: `T-WFBS-S` • **Livello**: `Standard` • **Tipo di contratto**: `Managed Service` • **Prodotto**: `WFBS-S` • **Tipo di configurazione**: `Spam Stats`

Prodotto/Servizio	Impostazioni
Worry-Free Business Security Advanced	• **Tipo**: `T-WFBS-A` • **Livello**: `Advanced` • **Tipo di contratto**: `Managed Service` • **Prodotto**: `WFBS-A` • **Tipo di configurazione**: `Spam Stats`
Worry-Free Business Security Services	• **Tipo**: `T-WFBSS` • **Livello**: `Standard` • **Tipo di contratto**: `Managed Service` • **Prodotto**: `WFBSS` • **Tipo di configurazione**: `Spam Stats`
Hosted Email Security	• **Tipo**: `T-HES` • **Livello**: `Standard` • **Tipo di contratto**: `Managed Service` • **Prodotto**: `HES` • **Tipo di configurazione**: `Spam Stats`

f. Fare clic su **Salva**.

8. Creare una nuova azienda per ciascun cliente da integrare in ConnectWise.

a. Accedere a **Contacts** > **Company** > **Nuovo**.

b. Modificare **Company ID**.

Si consiglia di utilizzare il nome cliente Remote Manager come ID dell'azienda per ConnectWise.

c. Fare clic su **Salva**.

Ripetere queste operazioni per creare un'azienda per ciascun utente.

9. Creare una nuova soluzione di gestione per ciascuna azienda

a. Fare clic su **Management (scheda)**.

b. Fare clic su **Salva**.

c. Fare clic su **New Item**.

d. Modificare **Solution** in `Remote Manager Management Solution`.

e. Modificare **Managed ID** nell'ID dell'azienda specificato nel passaggio precedente.

f. Fare clic su **Salva**.

10. Creare le configurazioni per ciascuna azienda.

a. Fare clic sulla scheda **Configuration**.

b. Creare una nuova configurazione impostando **Configuration Type** su `Spam Stats` e **Name** sull'D dell'azienda.

c. Fare clic su **Salva**.

11. Creare un nuovo contratto per ciascun cliente da integrare in ConnectWise.

a. Accedere alla scheda **Agreements** > **New**.

b. Selezionare `Managed Service` come **Agreement Type** e aggiornare gli altri dettagli come richiesto.

c. Fare clic su **Salva**.

12. Inserire aggiunte al contratto.

a. Accedere a **Agreements** > **Additions**.

b. Modificare i campi in base alle necessità.

Ad esempio, modificare il prezzo e il numero di serie.

Importante

per il numero di serie è necessario utilizzare il formato `SerialNumber: Serial_Company ID`.

---

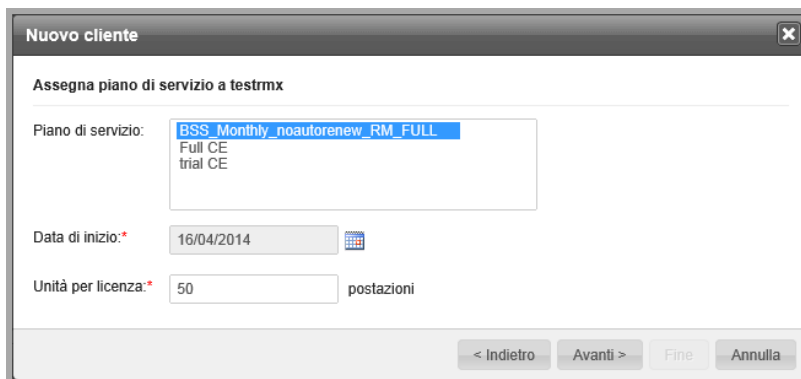
c. Fare clic su **Salva**.

Ripetere queste operazioni per ciascun prodotto/servizio gestito.

Capitolo 5

Gestione dei clienti

In questa sezione è trattato il seguente argomento:

Clienti

Nella pagina **Clienti** è possibile controllare i dettagli e le informazioni sulla licenza dei clienti. Sono inoltre disponibili le operazioni seguenti:

- Selezione del nome di ciascun cliente per visualizzarne le informazioni dettagliate
- Filtraggio dell'elenco clienti
- Esportazione delle informazioni dei clienti in un file CSV
- Aggiunta di nuovi clienti
- Rinnovo delle licenze
- Gestione dei prodotti

Aggiunta di nuovi clienti

Procedura

- Per gli account Licensing Management Platform:

  1. Accedere a **Clienti** > **{nome cliente}** > **Prodotti (scheda)** > **Aggiungi**.

  2. Selezionare il piano di servizio, la data di inizio e il numero di unità per licenza.

3. Fare clic su **Avanti**.

4. Configurare le impostazioni predefinite del prodotto. È possibile scegliere una delle seguenti opzioni:

Nota

Questa funzione viene visualizzata solo se è stato selezionato Worry-Free Business Security Services.

Assegna di piano servizio

Configura impostazioni predefinite prodotto

Base Modelli

Elenco approvati per reputazione Web e filtri URL

Quando si aggiungono URL, includere HTTP:// o HTTPS://. Aggiungi

http://www.trendmicro.com/*
http://wustat.windows.com/*
http://windowsupdate.microsoft.com/*
http://uk.trendmicro-europe.com/*

Elimina

Elenco bloccati per filtri URL

Quando si aggiungono URL, includere HTTP:// o HTTPS://. Aggiungi

Elimina

Attiva la scansione pianificata per il server

Giornaliero
Settimanale
Mensile

Ogni: Lunedì

Ora di inizio: 12 : 30
hh mm

Attiva la scansione pianificata per il dispositivo

Utilizza le impostazioni del server
Utilizza queste impostazioni:

Giornaliero
Settimanale
Mensile

Ogni: Lunedì

Ora di inizio: 12 : 30
hh mm

< Indietro Fine Annulla

- **Base**: consente di configurare solo le impostazioni visualizzate.
  - Elenco approvati per reputazione Web e filtri URL

    Nota
    Se si aggiunge un URL all'elenco approvato, accertarsi che non sia stato aggiunto all'elenco bloccato e viceversa.

  - Elenco bloccati per filtri URL
  - Scansione pianificata per server e dispositivo
- **Modelli**: Per impostare altre impostazioni utilizzando una console simile a Worry-Free Business Security, accedere a **Amministrazione** > **Configura modelli impostazione predefinita**.

5. Fare clic su **Fine**.

   Il prodotto/servizio viene aggiunto insieme e vengono visualizzati i relativi dettagli.

   Nota
   Annotare il GUID o la chiave di autorizzazione.

6. Per ottenere informazioni su come connettere il prodotto/servizio alla console, fare clic su **Connetti**.

- Per gli altri account:

1. Fare clic su **Nuovo cliente** nel banner oppure visitare la scheda **Clienti** > **Nuovo cliente**. Viene aperta la pagina Nuovo cliente.

2. Fornire le informazioni necessarie.

3. Fare clic su **Avanti >**.

4. Selezionare il tipo di prodotto e fornire una descrizione del prodotto.

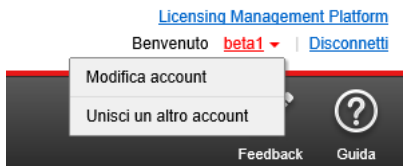
5. Fare clic su **Fine**.

Associazione di account

Se si gestiscono altri account Trend Micro Remote Manager che non sono stati migrati nella nuova Licensing Management Platform, è possibile unire tali account con quello corrente.

Procedura

1. Accedere a un account Remote Manager migrato in Licensing Management Platform.

   Viene visualizzata la schermata **Pannello di controllo**.

2. Fare clic sulla freccia accanto al nome di accesso e fare clic su **Unisci un altro account** > **Continua**.

AVVERTENZA!

Se si unisce un account a quello corrente, tutti i dati relativi a tale account vengono spostati. Se ad esempio attualmente si è eseguito l'accesso come `admin1` e si unisce `admin2` all'account `admin1`, tutti i dati dell'account `admin2` saranno eliminati dall'account `admin2`. Tali dati sono stati uniti all'account `admin1`. È sempre possibile aprire l'account `admin2`, ma tutti i dati risiedono nell'account `admin1`.

3. Immettere il nome utente e la password dell'account da unire a quello corrente.

4. Fare clic su **Unione**.

   Attendere un paio di minuti per consentire l'unione dei dati.

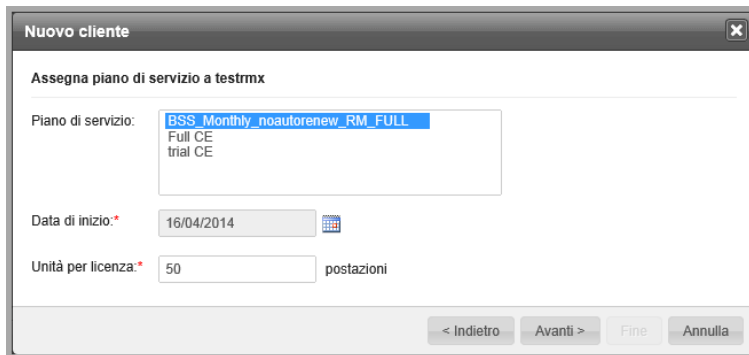
Operazioni successive

Dopo aver effettuato la migrazione dell'account, vengono visualizzate sempre le seguenti opzioni quando si aggiunge un nuovo cliente:

- **Con un account Licensing Management Platform attivo**: se il nuovo cliente dispone già di un account in Licensing Management Platform.

- **Con i server prodotto esistenti che richiedono la connessione a questo account**: se il nuovo cliente dispone di un prodotto o servizio, ma l'account non è stato integrato in Licensing Management Platform.

Verifica della licenza del prodotto

Verificare a cadenza regolare le licenze dei prodotti dei server gestiti dei clienti per garantire una protezione ininterrotta.

Procedura

1. Fare clic su **Clienti** > **{cliente}** > **{prodotto}** > **Licenza (scheda)**.
2. Verificare le informazioni sulla licenza del prodotto.

Aggiunta di prodotti/servizi

Procedura

1. Accedere a **Clienti** > **{nome cliente}** > **Prodotti (scheda)** > **Aggiungi**.
   - Per gli account Licensing Management Platform:
     a. Selezionare il piano di servizio, la data di inizio e il numero di unità per licenza.

     b. Aggiungere il prodotto o servizio.

     Il prodotto/servizio viene aggiunto insieme e vengono visualizzati i relativi dettagli.

c. Fare clic su **Fine**.

- Se si sta utilizzando un account integrato con Trend Micro Licensing Management Platform:

a. Selezionare il tipo di prodotto e aggiungere una descrizione del prodotto.

b. Fare clic su **Fine**.

c. Annotare il GUID o la chiave di autorizzazione. Sarà necessario al momento della *registrazione dei prodotti a pagina 4-8*.

Contatti

Se l'account è associato a Licensing Management Platform, è possibile aggiungere contatti, modificare le informazioni relative ai clienti o eliminare i contatti da Licensing Management Platform. Per svolgere queste azioni, fare clic sul collegamento a **Licensing Management Platform** sopra **Disconnetti**. Se non è presente il collegamento, è possibile visualizzare le informazioni relative ai clienti esclusivamente dalla console Web Remote Manager.

Aggiunta di contatti

Per l'iscrizione alle notifiche di eventi e ai rapporti, gli utenti dell'organizzazione del cliente devono prima essere aggiunti come contatti.

Nota

Se l'account è associato a Licensing Management Platform, fare clic sul collegamento a **Licensing Management Platform** sopra **Disconnetti** per aggiungere contatti. Se non è presente il collegamento, è possibile visualizzare le informazioni relative ai clienti esclusivamente dalla console Web Remote Manager.

Procedura

1. Accedere a **Clienti** > **{cliente}** > **Contatti (scheda)**.
2. Fare clic su **Aggiungi**.
3. Nella finestra **Aggiungi contatto**, inserire le seguenti informazioni:
   - Nome contatto
   - Numero di telefono
   - Codice postale
   - **E-mail**: Remote Manager invia notifiche degli eventi e rapporti a questo indirizzo.
   - Altro
4. Fare clic su **Salva**.

Modifica delle informazioni relative ai clienti

Le schede **Profilo azienda** e **Contatti** consentono di modificare le informazioni di un cliente.

Nota

Se l'account è associato a Licensing Management Platform, fare clic sul collegamento a **Licensing Management Platform** sopra **Disconnetti** per modificare le informazioni di contatto. Se non è presente il collegamento, è possibile visualizzare le informazioni relative ai clienti esclusivamente dalla console Web Remote Manager.

Procedura

1. Accedere a **Clienti** > **{cliente}** > **Profilo azienda (scheda)**.
2. Aggiornare le informazioni sull'azienda.

Nota

È inoltre possibile modificare il logo che viene visualizzato ogni volta che i clienti accedono alla console Web Remote Manager.

3. Accedere a **Clienti** > **{cliente}** > **Contatti (scheda)**.
4. Aggiornare i dettagli del contatto.
5. Fare clic su **Salva**.

Eliminazione di contatti

I clienti possono sottoscrivere notifiche e rapporti come contatti. Tuttavia, talvolta i contatti cambiano ed è necessario rimuoverne alcuni dall'elenco dei destinatari.

Nota

Se l'account è associato a Licensing Management Platform, fare clic sul collegamento a **Licensing Management Platform** sopra **Disconnetti** per modificare le informazioni di contatto. Se non è presente il collegamento, è possibile visualizzare le informazioni relative ai clienti esclusivamente dalla console Web Remote Manager.

Procedura

1. Accedere a **Clienti** > **{cliente}** > **Contatti (scheda)**.
2. Selezionare il contatto da eliminare.
3. Fare clic su **Elimina**.

Eliminazione di clienti

se si elimina un prodotto o servizio, verranno eliminati anche tutti i rispettivi record. Per registrare di nuovo il prodotto o servizio sul server Trend Micro Remote Manager, è necessario creare un nuovo GUID per il cliente. Sarà inoltre necessario reinstallare l'Agent Remote Manager sul prodotto gestito e utilizzare il nuovo GUID.

Nota

Questa funzione è applicabile solo agli account non integrati con Licensing Management Platform.

Procedura

1. Eliminare dal cliente tutti i prodotti/servizi associati.
    a. Fare clic su **Clienti** > **{cliente}**.
    b. Selezionare tutti i prodotti/servizi nella scheda **Prodotti**.
    c. Fare clic su **Elimina**.
2. Eliminare uno o più clienti.
    a. Fare clic su **Clienti**.
    b. Selezionare i clienti dall'elenco.

    Nota

    Selezionare esclusivamente i clienti che non dispongono di prodotti o servizi.

    c. Fare clic su **Elimina**.

Filtraggio dell'elenco clienti

L'elenco clienti può essere lungo o corto, a seconda del numero dei clienti. Per ottenere le informazioni necessarie, è possibile restringere il numero dei clienti e cercare solo i clienti che corrispondono al profilo impostato.

Procedura

1. Nella console Web Remote Manager fare clic su **Clienti**.

   Tutti i clienti vengono visualizzati su questa pagina.

2. A destra, selezionare uno o più campi.

   Nota

   Se si seleziona più di un (1) campo, con ogni probabilità si ottengono le informazioni necessarie e questo è un aspetto positivo. È tuttavia possibile escludere le informazioni necessarie, pertanto è opportuno prestare attenzione a ciò che si seleziona.

3. (Facoltativo) Fare clic su **Esporta** per generare un file CSV dei clienti filtrati.

Capitolo 6

Gestione degli Agent

In questa sezione sono trattati i seguenti argomenti:

Gestione degli Agent dalla console Web Remote Manager

Questa sezione contiene informazioni relative alla modalità di gestione degli Agent dalla console Web Trend Micro™ Remote Manager™.

Controllo della connessione tra Agent e server

Per garantire che il servizio Trend Micro Remote Manager sia in esecuzione senza problemi, verificare che lo stato degli Agent visualizzato nella console Remote Manager sia "connesso" o "online".

Accedere a **Clienti** > **{cliente}** > **Prodotti (scheda)**.

Nella colonna **Stato** della struttura è indicato lo stato di ciascun Agent. Per informazioni su ogni stato, vedere *Stato dell'Agent a pagina 6-2*.

Oltre alla sezione corrente, fare riferimento a *Risoluzione dei problemi e problemi noti a pagina 11-1* per ulteriori problemi relativi alla connettività server/Agent.

Stato dell'Agent

Lo stato di un Agent Remote Manager indica se l'Agent è in grado di raccogliere i dati e ricevere i comandi dal server Remote Manager. Lo stato indica anche il motivo per cui l'Agent non può funzionare correttamente e come è possibile gestire la situazione. Nella tabella riportata di seguito sono descritti i tipi di stato dell'Agent e i modi per gestire la situazione.

TABELLA 6-1. Tipi di stato dell'Agent

STATO	DESCRIZIONE	RISOLUZIONE
Online	L'Agent è in esecuzione normalmente.	N/D

Stato	Descrizione	Risoluzione
Anomalo	L'Agent sembra essere non in linea e non risponde al server Remote Manager, ma non è stata inviata una richiesta di disconnessione.	Questo stato può essere in atto se il server gestito non è stato arrestato correttamente. Verificare che l'amministratore del server gestito sia a conoscenza della situazione. Contattare l'amministratore, se necessario.
Disattivato	Questo stato viene impostato manualmente dalla console. Quando un Agent è nello stato disattivato, l'Agent riceve i comandi dal server ogni 10 minuti.	Inviare un comando per attivare l'Agent (vedere *Inoltro di comandi all'Agent a pagina 6-4*).
Offline	L'Agent è stato chiuso normalmente dopo aver inviato una richiesta di disconnessione al server Remote Manager. In genere, un Agent si trova in questo stato se un utente ha chiuso il servizio Agent o se il server gestito è stato arrestato.	Verificare che l'amministratore del server gestito sappia che il server è stato arrestato. Contattare l'amministratore del server gestito, se necessario.
Sconosciuto	L'Agent non funziona normalmente.	Rimuovere l'Agent e farlo reinstallare dall'amministratore del server gestito. Se il problema persiste, contattare il fornitore del supporto.
Errori plug-in	La console ha rilevato errori nel componente plug-in del servizio dell'Agent.	Rimuovere l'Agent e chiedere all'amministratore del server gestito di reinstallarlo. Se il problema persiste, contattare il fornitore del supporto.
Non registrato	L'Agent non è stato registrato sul server Remote Manager.	L'Agent potrebbe non essere stato installato o non è in grado di comunicare correttamente con il server Remote Manager. Contattare l'amministratore del server gestito.

STATO	DESCRIZIONE	RISOLUZIONE
Versioni non corrispondenti	È stata rilevata un'incompatibilità tra le versioni dei seguenti componenti: • Agent • Remote Manager • Worry-Free Business Security (Standard e Advanced)	Aggiornare l'Agent e il server gestito. Se non funziona, segnalare il problema all'amministratore di Trend Micro Data Center.

Inoltro di comandi all'Agent

I comandi dell'Agent consentono di risolvere in remoto i problemi che interessano l'Agent Worry-Free Business Security (Standard e Advanced). Se un Agent si trova nello stato anomalo o non registrato, non è possibile inviare un comando a tale Agent.

Procedura

1. Accedere a **Clienti** > **{clienti}** > **{prodotto}** > **Gruppi (scheda)**.

   Selezionare uno dei comandi riportati di seguito:

   - **Esegui scansione**: permette di avviare una scansione dell'endpoint.
   - **Arresta scansione**: interrompe il processo di scansione.

2. Accedere a **Clienti** > **{clienti}** > **{prodotto}** > **Impostazioni dominio (scheda)**.

   Selezionare uno dei comandi riportati di seguito:

   - **Attiva**: ripristina l'Agent dallo stato disattivato alla funzionalità normale.
   - **Disattiva**: l'Agent smette di raccogliere informazioni ma continua a richiedere comandi al server ogni 10 minuti.
   - **Avvia valutazione delle vulnerabilità**: esegue una scansione per la valutazione delle vulnerabilità.

- **Avvia Damage Cleanup Services**: esegue la scansione e disinfetta il computer da virus di rete e basati su file e dai residui di worm e virus.

3. Accedere a **Clienti** > **{clienti}** > **{prodotto}** > **Server gestito (scheda)**.

   Selezionare uno dei comandi riportati di seguito:

   - **Aggiorna server gestito**: permette di scaricare e installare gli aggiornamenti del server gestito.
   - **Aggiorna Security Agent**: permette di scaricare e installare gli aggiornamenti dell'Agent.

Visualizzazione dei dettagli dell'Agent

Procedura

1. Accedere a **Clienti** > **{cliente}** > **Prodotti (scheda)** > **WFBS-S/WFBS-A** > **Endpoint**.

   Vengono visualizzate le informazioni seguenti:

   - **Stato**
   - **Nome**
   - **GUID**: identificatore univoco globale; è una stringa generata automaticamente da Remote Manager. Comunicare il GUID all'amministratore che installerà il programma Agent.
   - **Indirizzo IP**: indirizzo IP del server in cui è installato l'Agent.
   - **Registrato il**
   - **Ultimo aggiornamento**: data e ora dell'ultimo aggiornamento dell'Agent
   - **Versione Agent**
   - **Prodotto gestito**: prodotto gestito tramite l'Agent

- **Versione prodotto gestito**: versione del prodotto gestito tramite l'Agent

Gestione degli Agent dal server gestito

In questa sezione sono fornite informazioni su come gestire gli Agent dal server gestito.

Messaggi di stato dell'Agent

Sul server gestito, l'Agent visualizza una delle seguenti icone sulla barra delle applicazioni:

TABELLA 6-2. Icone sulla barra delle applicazioni

ICONA	DESCRIZIONE
	Un'icona verde indica che l'Agent è connesso al server di comunicazione di Remote Manager. L'Agent funziona normalmente.
	Un'icona rossa indica che l'Agent non è connesso al server di comunicazione di Remote Manager o che la versione dell'Agent non corrisponde al server ed è necessario aggiornarla.
	Un'icona con una freccia rossa indica che l'Agent è stato disconnesso da Remote Manager.
	Un'icona con una X rossa indica che l'Agent è stato disconnesso.

Modifica del GUID dell'Agent sul server gestito

Se si è immesso un identificatore univoco globale (GUID) errato durante l'installazione dell'Agent Remote Manager, eliminare l'Agent e installarlo di nuovo utilizzando il GUID corretto. Se questa procedura dovesse risultare impossibile, procedere come indicato:

Procedura

1. Accedere a `C:\Programmi\Trend Micro\TMRMAgentForCSM`.

2. Aprire il file `AgentSysConfig.xml` utilizzando un editor di testo.
3. Cercare il GUID tra i parametri `<AgentGUID>` e `</AgentGUID>`.
4. Modificare il GUID e salvare il file.
5. Nella stessa cartella, aprire il file `csmSysConfig.xml` utilizzando un editor di testo.
6. Cercare il GUID tra i parametri `<ProductGUID>` e `</ProductGUID>`.
7. Modificare il GUID e salvare il file.
8. Fare clic destro sull'icona dell'Agent Trend Micro Remote Manager sulla barra delle applicazioni, quindi fare clic su **Riavvia servizio**.

Uso dell'Agent Configuration Tool

Agent Configuration Tool consente di apportare modifiche alle impostazioni di configurazione dell'Agent Remote Manager.

Accedere a **Start** > **Programmi** > **Trend Micro Remote Manager Agent** > **Agent Configuration Tool** oppure fare clic con il pulsante destro del mouse sull'icona sulla barra delle applicazioni e fare clic su **Configura**.

Per ulteriori informazioni, consultare la sezione *Configurazione dell'Agent a pagina 6-8*.

Configurazione dell'Agent

Menu di configurazione dell'Agent

Per configurare l'Agent, fare clic con il pulsante destro del mouse sull'icona sulla barra delle applicazioni per aprire il seguente menu:

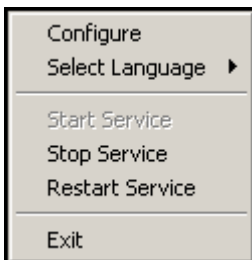



FIGURA 6-1. Menu a comparsa di Agent Configuration Tool

Vengono visualizzate le seguenti voci:

- **Configura**: consente di aprire la schermata di configurazione dell'Agent.
- **Seleziona lingua**: oltre ad altre lingue possibili, la lingua inglese è sempre presente.
- **Servizio**: consente l'avvio, l'arresto e il riavvio.
- **Esci**: L'uscita dallo strumento non provoca l'arresto del servizio Remote Manager, ma semplicemente la chiusura di Agent Configuration Tool e la rimozione dell'icona dalla barra delle applicazioni. Lo strumento può essere riavviato in qualsiasi momento.

Finestra di dialogo principale dello strumento di configurazione

Fare clic con il pulsante destro del mouse sull'icona sulla barra delle applicazioni e selezionare **Configura** nel menu di configurazione dell'Agent per aprire la scheda **Generale** dello strumento di configurazione.

FIGURA 6-2. Scheda Generale di Agent Configuration Tool

Le seguenti sezioni della schermata di configurazione dell'Agent sono le uniche attualmente rilevanti dello strumento.

- **Impostazioni server**: Per configurare la comunicazione del server, effettuare le seguenti impostazioni:
    - **Indirizzo server**: Il nome di dominio completo (FQDN) del server di comunicazione di Remote Manager. Il valore FQDN dipende dall'area geografica, come indicato di seguito:
        - **Asia Pacifico**: `rm-apaca.trendmicro.com`
        - **Europa e Medio Oriente:** `rm-emea.trendmicro.com`
        - **Giappone**: `rm-jpa.trendmicro.com`
        - **America Latina**: `rm-lara.trendmicro.com`
        - **Nord America**: `rm-usa.trendmicro.com`
    - **Porta**: La porta che il server Remote Manager utilizza per comunicare con l'Agent. Dovrebbe essere 80 per HTTP e 443 per HTTPS.
    - **Protocollo**: il protocollo utilizzato per la comunicazione tra il server e l'Agent.
- **Impostazioni server proxy**: Attivare l'area selezionando la casella di controllo **Impostazioni server proxy** se la rete dell'utente richiede un proxy per comunicare con il server Remote Manager.
    - **Indirizzo**: l'indirizzo IP del server proxy.
    - **Porta**: la porta o il server proxy
    - **Protocollo**
- **Pulsante Test di connessione**: Il pulsante **Test di connessione** consente di eseguire il test della comunicazione tra l'Agent e il server Remote Manager. Utilizzare questa funzione per verificare il funzionamento della connessione di base al server di comunicazione. Se non riesce (viene visualizzata una finestra di dialogo a comparsa se lo strumento non può connettersi al server), potrebbe sussistere un problema di base, legato ad esempio all'indirizzo del server di comunicazione e alla relativa porta o all'indirizzo del server proxy e alla relativa porta.

Backup e ripristino delle impostazioni dell'Agent

Per disinstallare e reinstallare l'Agent utilizzando lo stesso GUID in un intervallo di tre giorni, mantenere le impostazioni dell'Agent onde evitare la sovrapposizione di dati. A tal fine, eseguire il backup manuale dei file di configurazione, quindi sostituire i file di configurazione con la copia di backup dopo la reinstallazione dell'Agent.

Backup delle impostazioni

Procedura

1. Sul server gestito, fare clic con il pulsante destro del mouse sull'icona dell'Agent sulla barra delle applicazioni e selezionare **Arresta servizio** per arrestare il servizio Agent.
2. Copiare tutti i file `.xml`, `.dat` e `.ini` dalla cartella di installazione `C:\Programmi\ Trend Micro\WFRMAgentforCSM`.
   - File `.xml`
     - `csmSysConfig.xml`
     - `csmLocalConfig.xml`
     - `csmLogDef.xml`
     - `AgentWorkConfig.xml`
     - `AgentSysConfig.xml`
     - `AgentStatus.xml`
     - `AgentLocalConfig.xml`
   - File `.dat`
     - `MSA.dat`
     - `logBuf.dat`

- `group.dat`
        - `CSA.dat`
        - `CriticalVA.dat`
    - File `.ini`
        - `csmStatusData.ini`
3. Copiare tutti i file dalla cartella `\Cache`.
4. Riavviare il servizio Agent.

Ripristino delle impostazioni

Procedura

1. Rimuovere l'Agent in locale, se l'operazione non è già stata eseguita. Per istruzioni dettagliate, vedere *Rimozione degli Agent in locale a pagina 6-15*.

    Nota

    durante la rimozione dell'Agent in locale, viene annullata la registrazione dell'Agent in Remote Manager e vengono automaticamente eliminati tutti i dati associati all'Agent. Per evitare l'annullamento della registrazione dell'Agent, modificare il valore Indirizzo server nell'interfaccia dell'Agent prima di rimuovere l'Agent.

    ---

2. Reinstallare l'Agent. Assicurarsi di utilizzare lo stesso GUID, che può essere ottenuto da `AgentSysConfig.xml`.
3. Sul server gestito, fare clic con il pulsante destro del mouse sull'icona dell'Agent sulla barra delle applicazioni e selezionare **Arresta servizio** per arrestare il servizio Agent.
4. Sostituire i file di configurazione con i file di backup.
5. Fare clic con il pulsante destro del mouse sull'icona dell'Agent sulla barra delle applicazioni e selezionare **Avvia servizio** per riavviare il servizio Agent.

Individuazione del numero di build dell'Agent

Il numero di build dell'Agent può essere verificato sia dalla console che direttamente sull'Agent.

Dalla console Web Remote Manager

Procedura

1. Fare clic sulla scheda **Clienti**.
2. Selezionare il dominio di destinazione dall'elenco a discesa **Visualizza per** nel riquadro sinistro.
3. Fare clic su **Tutti i clienti** > **{cliente}** > **{Agent}** > **Dettagli server/Agent** > **Dettagli Agente TMRM**.
4. Verificare la versione dell'Agent nella tabella **Informazioni generali**.

Sull'Agent

Procedura

1. Andare alla directory `C:\Program Files\Trend Micro\WFRMAgentForCSM`.
2. Fare clic con il pulsante destro del mouse sul file `csmplugin.dll`, quindi fare clic su **Proprietà** > **Versione (scheda)** per vedere il numero di build.

Posizione dei registri dell'Agent e dei file di configurazione

I file di configurazione dell'Agent si trovano in:

- `<percorso di installazione>\Trend Micro\WFRMAgentForCSM \*.xml`
- `<percorso di installazione>\Trend Micro\WFRMAgentForCSM \*.ini`

I file di registro si trovano in:

- `<percorso di installazione>\Trend Micro\WFRMAgentForCSM\log \`

Attivazione del registro di debug dell'Agent

In genere, l'Agent registra solo avvisi e informazioni sugli errori. Se sono necessarie ulteriori informazioni sul registro, attivare il registro di debug dell'Agent.

Risoluzione

1. Aprire il file `AgentLocalConfig.xml` in `<install path>\Trend Micro \WFRMAgentForCSM\` in un editor di testo.
2. Modificare `<DebugLogLevel>` da `LL_FOR_ERROR` a `LL_FOR_ALL`.
3. Riavviare il servizio dell'Agent facendo clic con il pulsante destro del mouse sull'Agent Remote Manager nella barra delle applicazioni, quindi facendo clic su **Riavvia servizio**.
4. Il file di registro dell'Agent è `<install path>\Trend Micro \WFRMAgentForCSM\log\TMICAgent.log`.

Rimozione degli Agent

In questa sezione sono fornite informazioni su come rimuovere gli Agent.

Rimozione degli Agent in locale

Prima di rimuovere l'Agent, consultare *Backup e ripristino delle impostazioni dell'Agent a pagina 6-11*.

AVVERTENZA!

Se si annulla la registrazione di un Agent da Remote Manager, vengono eliminati tutti i dati associati all'Agent Remote Manager. Per evitare l'annullamento della registrazione dell'Agent (e la conseguente eliminazione dei rispettivi dati), modificare il valore dell'indirizzo del server nell'interfaccia dell'Agent Remote Manager prima di rimuovere l'Agent Remote Manager.

Esistono tre modi per rimuovere un Agent Remote Manager in locale:

- Disinstallare direttamente l'Agent Remote Manager.
- Disinstallare l'Agent Remote Manager dal Pannello di controllo.
- Disinstallare l'Agent Remote Manager manualmente.

Disinstallazione diretta dell'Agent Remote Manager

Procedura

1. Aprire il file di installazione dell'Agent Remote Manager (`WFRMAgentforCSM.exe` o `WFRMAgentforWFBS.exe`).
2. Fare clic su **Sì** nella finestra di dialogo **Conferma disinstallazione**.

   Nota

   Durante la rimozione, viene richiesto di chiudere determinate applicazioni. Chiudere tali applicazioni e scegliere **Riprova** per continuare.

3. Al termine della disinstallazione, fare clic su **Fine** per chiudere la procedura guidata.

Disinstallazione dell'Agent Remote Manager dal pannello di controllo

Procedura

1. Aprire l'applet **Installazione applicazioni** del Pannello di controllo (oppure **Programmi e impostazioni** in Windows Vista™).
2. Selezionare `Trend Micro Remote Manager Agent` e fare clic sul pulsante **Modifica/Rimuovi**.
3. Seguire le istruzioni visualizzate.

Disinstallazione manuale dell'Agent Remote Manager

Se per qualche motivo un Agent non può essere rimosso tramite la procedura standard, eseguire questi passaggi:

Procedura

1. Arrestare il servizio dell'Agent Remote Manager.
   a. Accedere a **Start** > **Esegui**.
   b. Digitare `cmd` nella riga di comando, quindi premere **Invio**.
   c. Eseguire il seguente comando:

   ```
   net stop Trend Micro Worry-Free Remote Manager Agent
   ```

2. Rimuovere il servizio dell'Agent Remote Manager:
   a. Nella riga di comando, utilizzare il comando di cambio directory (cd) per passare alla directory dell'Agent Remote Manager.
   b. Eseguire il seguente comando:

   ```
   TMICAgent -u
   ```

3. Rimuovere i file del programma.

```
Delete {Agent install directory} / WFRMAgentForCSM
```

4. Aprire l'Editor del Registro di sistema (`regedit.exe`) e rimuovere le seguenti chiavi di registro:

Nota

Effettuare sempre un backup prima di modificare il Registro. Modifiche errate al Registro di sistema potrebbero provocare problemi gravi. Nel caso ciò dovesse accadere, eseguire un ripristino come illustrato nell'argomento della Guida "Ripristino del Registro di sistema" in `regedit.exe` o "Ripristino di una chiave del Registro di sistema" in `regedt32.exe`.

- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TMIC4CSM\Agent \HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Products \23FC8F347B51DD440AD13A73D13A73D22D58E6`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion\Installer\UserData\S-1-5-18\Products \23FC8F347B51DD440AD13A73D13A73D22D58E6`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion\Uninstall\{43F8CF32-15B7-44DD-A01D-A3372DD2856E}`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion\Uninstall\InstallShield Uninstall Information\{43F8CF32-15B7-44DD-A01D-A3372DD2856E}`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion\Uninstall\InstallShield_ \{43F8CF32-15B7-44DD-A01D-A3372DD2856E}`

5. Rimuovere il collegamento all'Agent Remote Manager dal menu Start.

   a. Sul desktop, fare clic su **Risorse del computer**.

   b. Modificare la directory corrente in `..\Documents and Settings\All Users\Menu Start\Programmi`.

c. Eliminare la cartella dell'Agent Remote Manager.

Capitolo 7

Gestione delle licenze

In questa sezione sono trattati i seguenti argomenti:

Nota

Questa funzione è applicabile solo se si utilizza un account integrato con Trend Micro Licensing Management Platform.

Aggiunta di allocazioni delle postazioni

Ogni rivenditore può specificare il numero di postazioni che può allocare per cliente. Se superano il numero di postazioni allocato, i rivenditori possono aggiungere altre postazioni per cliente.

Nota

Questa funzione è applicabile solo se si utilizza un account integrato con Trend Micro Licensing Management Platform.

Procedura

1. Esistono vari modi per visualizzare la finestra **Aggiungi postazioni**:
   - Nella console Web Trend Micro™ Remote Manager™:
     a. Fare clic su **Clienti**.
     b. Selezionare il cliente che ha superato il limite di allocazione delle postazioni.
     c. Fare clic su **Modifica postazioni**.
   - Nel widget **Notifiche**, fare clic sul collegamento **Aggiungi postazioni adesso** situato accanto alla notifica.
   - Nel messaggio di notifica, fare clic sul pulsante **Aggiungi postazioni adesso**.
2. Specificare il numero di postazioni da aggiungere all'allocazione.
3. Fare clic su **Invia**.

Rinnovo delle licenze

È possibile rinnovare le licenze dei clienti gestiti.

Nota

Questa funzione è applicabile solo se si utilizza un account integrato con Trend Micro Licensing Management Platform.

Procedura

1. Esistono vari modi per visualizzare la finestra **Rinnovo licenze**:
    - Nella console Web Remote Manager:
        a. Fare clic su **Clienti**.
        b. Selezionare il cliente la cui licenza è scaduta o è prossima alla scadenza.
        c. Fare clic su **Rinnovo licenza**.
    - Nel widget **Notifiche**, fare clic sul collegamento **Rinnova adesso** situato accanto alla notifica.
    - Nel messaggio di notifica, fare clic sul pulsante **Rinnova adesso**.
2. Specificare la modifica ai termini della licenza.
3. Fare clic su **Invia**.

Capitolo 8

Gestione delle impostazioni

In questa sezione sono trattati i seguenti argomenti:

Configurazione delle notifiche

Impostare le notifiche per eventi che richiedono attenzione. Tali notifiche possono essere inviate sotto forma di messaggi e-mail, dal widget **Notifiche**, oppure mediante software di terzi.

Procedura

1. Configurare le impostazioni di notifica generali.

    a. Fare clic su **Amministrazione** > **Configura notifiche**.

    Nota

    Nella schermata visualizzata è indicato l'indirizzo e-mail che riceverà la notifica. Se l'indirizzo non è corretto, visitare la pagina **Account** o la console Web Licensing Management Platform e modificare le impostazioni del profilo.

    b. Selezionare la lingua.

    c. (Facoltativo) Attivare o disattivare il messaggio e-mail di riepilogo giornaliero delle notifiche. In tal modo si riceve ogni giorno un messaggio e-mail di notifica grazie al quale è possibile rimanere informati su tutti gli eventi attivati e che continuano a richiedere attenzione.

    d. Specificare i tipi di notifiche che vengono inviate all'attivazione degli eventi:

    - **Mostra nelle notifiche**: per l'evento specificato vengono visualizzate le notifiche nel widget corrispondente. Nell'icona Notifiche sulla sezione corrispondente al banner della console viene visualizzato anche il numero di eventi.

    - **E-mail:** per l'evento specificato si riceve una notifica e-mail. Dai collegamenti forniti in questo messaggio e-mail potrebbe essere possibile rinnovare direttamente le licenze o aggiungere le postazioni allocate.

    e. Fare clic su **Salva**.

2. Configurare le impostazioni di notifica specifiche per i clienti.

    a. Accedere a **Cliente** > **{nome cliente}** > **Notifiche (scheda)**.

b. Selezionare l'impostazione di notifica.

c. Specificare ulteriori destinatari.

Nota

Accertarsi che i clienti abbiano integrato gli strumenti di terzi prima di attivare le notifiche per Kaseya, Autotask o ConnectWise.

Configurazione delle impostazioni della console

Specificare il logo che viene visualizzato ogni volta che i clienti accedono al servizio.

Nota

Questa impostazione è facoltativa.

Procedura

1. Fare clic su **Amministrazione** > **Impostazioni console**.
2. Selezionare l'immagine da utilizzare. Il logo deve essere un'immagine `.png`, `.jpg`, `.bmp` o `.gif` con dimensioni consigliate di 600 x 55 pixel (larghezza x altezza).
3. Fare clic su **Salva**.

Configurazione dei modelli di impostazione predefinita

Nota

I modelli di impostazione predefinita sono disponibili esclusivamente se si integra Trend Micro Remote Manager con Licensing Management Platform e solo per il prodotto Worry-Free Business Security Services.

I modelli di impostazione predefinita contengono impostazioni cliente preconfigurate. In tal modo è più semplice assicurarsi che i clienti utilizzino le stesse impostazioni.

Quando si creano i modelli, viene visualizzata una console con interfaccia simile a Worry-Free Business Security Services; ciò consente una maggiore familiarità durante l'impostazione delle opzioni predefinite utilizzabili da ciascun cliente. È possibile creare diversi modelli specifici per tipi o gruppi di clienti.

Per ulteriori informazioni sulle impostazioni che è possibile configurare da questo modello, consultare la documentazione di Worry-Free Business Security Services all'indirizzo:

http://docs.trendmicro.com/it-it/smb/worry-free-business-security-services.aspx

Procedura

1. Accedere a **Amministrazione** > **Configura modelli impostazione predefinita**.
2. Fare clic su **Crea**.

3. Specificare il nome del modello e alcuni commenti o descrizioni in modo da ricordare in seguito la funzione o il destinatario di tale modello.

4. Fare clic su **Configura modello**.

Nota

Si apre una console simile a Worry-Free Business Security Services. Tutte le modifiche apportate a questo sito vengono salvate come modello e non hanno alcun effetto sui prodotti registrati.

5. Configurare le seguenti impostazioni:

- Criteri

  a. Accedere a **Dispositivi** > **Server (predefinito)** > **Configura criteri**.

  b. Configurare le impostazioni dei criteri del server predefinito.

  c. Accedere a **Scansioni** > **Dispositivo (predefinito)** > **Configura criteri**.

  d. Configurare le impostazioni dei criteri del dispositivo predefinito.

e. Fare clic su **Salva**.

- Impostazioni di scansione

a. Accedere a **Scansioni** > **Scansione manuale (scheda)**.

b. Configurare le impostazioni di server e dispositivo predefiniti.

c. Accedere a **Scansioni** > **Scansione pianificata (scheda)**.

d. Configurare le impostazioni di server e dispositivo predefiniti.

e. Fare clic su **Salva**.

- Impostazioni di notifica

a. Accedere a **Amministrazione** > **Notifiche** > **Eventi (scheda)**.

b. Specificare gli eventi e i destinatari che attivano una notifica degli eventi.

c. Fare clic su **Salva**.

- Impostazioni globali

a. Accedere a **Amministrazione** > **Impostazioni globali** > **Impostazioni di sicurezza (scheda)**.

b. Apportare le dovute modifiche alle impostazioni relative a scansione, monitoraggio del comportamento o prevenzione delle infezioni.

c. Accedere a **Amministrazione** > **Impostazioni globali** > **Impostazioni di approvati/bloccati (scheda)**.

d. Aggiungere o rimuovere siti approvati o bloccati.

e. Accedere a **Amministrazione** > **Impostazioni globali** > **Controllo Agent (scheda)**.

f. Modificare le impostazioni dell'Agent.

g. Accedere a **Amministrazione** > **Impostazioni globali** > **Gestione dispositivo (scheda)**.

h. Modificare le impostazioni di gestione del dispositivo basato sull'utente.

i. Fare clic su **Salva**.

Capitolo 9

Gestione degli eventi

In questa sezione sono trattati i seguenti argomenti:

Gestione degli eventi

In Trend Micro Remote Manager, un evento si verifica quando un prodotto o servizio nella postazione di un cliente necessita di attenzione. Per esaminare e gestire gli eventi di tutti i clienti, utilizzare la schermata **Registri incidenti**. È possibile cercare gli eventi che si sono verificati in Worry-Free Business Security, Worry-Free Business Security Services e Hosted Email Security in base al tipo o al cliente. È inoltre possibile filtrare gli eventi per gravità e stato.

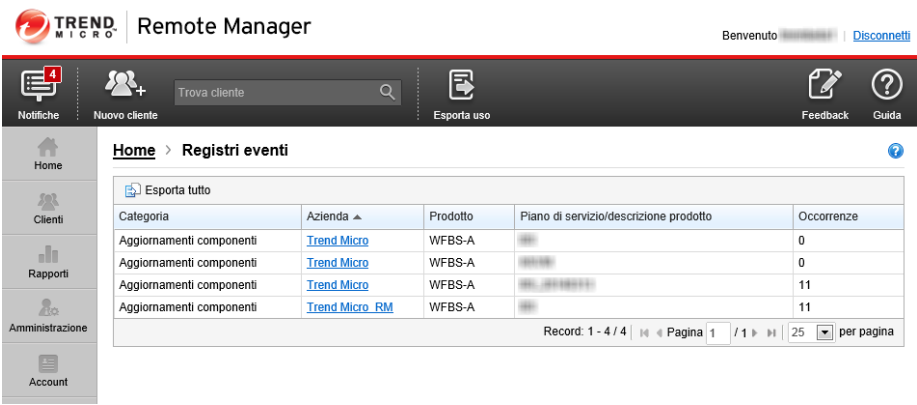



FIGURA 9-1. Schermata Registri incidenti che mostra eventi antivirus

Eventi

Gli eventi sono classificati in base alle seguenti categorie:

- Minacce
  - *Difesa dalle infezioni a pagina 9-5*
  - *Antivirus a pagina 9-7*
  - *Anti-spyware a pagina 9-9*
  - *Anti-spam a pagina 9-11*
  - *Virus di rete a pagina 9-11*

- *Reputazione Web a pagina 9-12*
    - *Monitoraggio del comportamento a pagina 9-13*
    - *Filtri URL a pagina 9-13*
    - *Controllo dispositivi a pagina 9-14*

- Sistema

    - *Smart Protection Service a pagina 9-14*
    - *Aggiornamento dei componenti a pagina 9-15*
    - *Uso del disco a pagina 9-16*

- Licenza
    - Licenza scaduta
    - Licenza in scadenza
    - Utilizzo postazione

Gravità

La gravità viene classificata in base alle seguenti categorie:

- **Operazione richiesta**: eventi che richiedono attenzione immediata.
- **Avviso**: gli avvisi e le notifiche hanno solo scopo informativo.

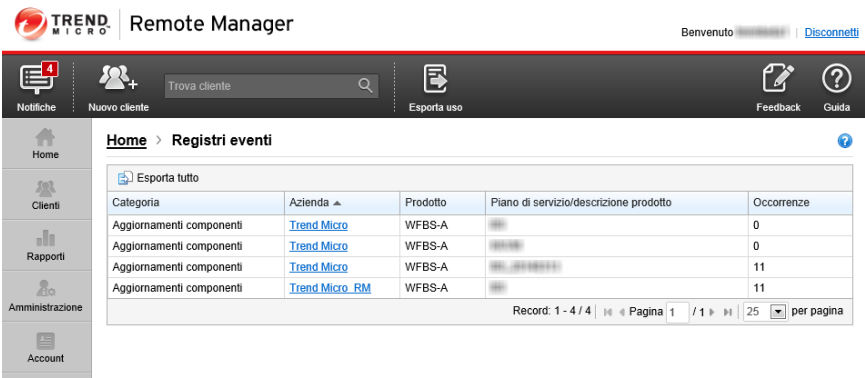
Stato

Lo stato viene classificato in base alle seguenti categorie:

- **Non risolto**: eventi che richiedono attenzione.
- **Reimpostazione/Aggiornamento**: eventi sui quali si è intervenuti che attendono un aggiornamento da parte del prodotto/servizio.

Visualizzazione degli eventi

Procedura

1. Accedere a **Home** > **{pannello di controllo}** > **{widget}**
2. Fare clic su uno degli incidenti.

3. Effettuare una delle seguenti operazioni:
   - Visualizzare gli incidenti in base al tipo o al cliente mediante la struttura e la finestra di ricerca sulla sinistra
   - Visualizzare gli eventi relativi a un particolare prodotto/servizio mediante le schede sulla destra
   - Filtrare gli eventi in base alla gravità o allo stato mediante gli elenchi a discesa in alto a destra della schermata
   - Eseguire il drill-down di un evento particolare facendo clic sui collegamenti dai widget o dalle notifiche per visualizzare ulteriori informazioni
   - Selezionare un evento, quindi fare clic su **Reimposta** per reimpostare il conteggio o su **Aggiorna** per aggiornare i componenti.

Per informazioni su ciascun evento e sulle azioni da compiere, consultare la sezione *Tipi di eventi a pagina 9-5*.

Tipi di eventi

Qui sono indicati i vari tipi di evento che è possibile visualizzare in Trend Micro Remote Manager.

Dettagli sullo stato di difesa dalle infezioni

Nota

Questa funzione è disponibile solo per Worry-Free Business Security (tutti).

Difesa dalle infezioni fornisce avvisi tempestivi per minacce Internet e altre minacce informatiche di portata globale. Questa funzione risponde automaticamente con misure preventive che garantiscono la sicurezza dei computer e della rete, seguite da misure di protezione volte a identificare il problema e risanare il danno. Mentre Difesa dalle infezioni protegge la rete e i client, *TrendLabs a pagina 12-5* è impegnato a creare soluzioni contro la minaccia. Dopo aver sviluppato la soluzione, TrendLabs rilascia componenti aggiornati che vengono scaricati e implementati nei client dai server Worry-Free Business Security (tutti). Difesa dalle infezioni disinfetta quindi i residui di virus e ripara i file e le directory danneggiati dalla minaccia.

In caso di infezione, Difesa dalle infezioni può adottare le seguenti misure:

- Blocco delle porte
- Protezione da scrittura di determinati file e directory
- Blocco di determinati allegati

Per determinare lo stato di difesa dalle infezioni per le reti gestite, Trend Micro controlla se TrendLabs ha dichiarato un avviso di virus. Nel pannello di controllo viene visualizzato un evento di difesa dalle infezioni solo se si è verificato almeno un evento di questo tipo.

Nella tabella riportata di seguito sono illustrate le possibili icone di stato di difesa dalle infezioni.

TABELLA 9-1. Icone di stato di difesa dalle infezioni

ICONA DI STATO	DESCRIZIONE
	TrendLabs ha dichiarato un allarme giallo.
	TrendLabs ha dichiarato un allarme rosso.

Stato di avviso

Le informazioni sullo stato di avviso vengono visualizzate in caso di allarme rosso o giallo. Attivare Difesa dalle infezioni per garantire che le misure preventive vengano applicate automaticamente per proteggere la rete prima che diventi disponibile un pattern.

Computer vulnerabili

I computer vulnerabili sono computer che non dispongono delle patch per vulnerabilità software note. Per gestire i computer vulnerabili, contattare l'amministratore del dominio interessato e specificare i nomi dei computer vulnerabili, insieme alle vulnerabilità che li affliggono. Per ottenere queste informazioni, fare clic sul numero di computer vulnerabili.

Per avere la certezza che l'elenco di computer vulnerabili sia aggiornato, eseguire una scansione di valutazione delle vulnerabilità (VA). Per ulteriori informazioni, fare riferimento a *Comandi di Worry-Free Business Security a pagina 3-27*.

Computer da disinfettare

I computer da disinfettare sono computer che hanno subito un'infezione da virus o minaccia informatica che il client di protezione non è stato in grado di disinfettare, eliminare o mettere in quarantena dopo il rilevamento. In genere, un computer infetto contiene una copia in esecuzione della minaccia informatica o del virus, che ha configurato il computer in modo da consentire l'avvio e l'esecuzione automatica.

Per visualizzare un elenco dei computer infetti e dei nomi dei virus, fare clic sul numero di computer da disinfettare. Per gestire i computer infetti, implementare Damage Cleanup Services (DCS) nel dominio. Per ulteriori informazioni, fare riferimento a *Comandi di Worry-Free Business Security a pagina 3-27*.

Dettagli sullo stato antivirus

Nota

Questa funzione è disponibile solo per Worry-Free Business Security (tutti).

Nella tabella riportata di seguito sono descritte le possibili icone di stato antivirus con i colori associati.

TABELLA 9-2. Icone di stato antivirus

ICONA DI STATO	DESCRIZIONE
	Questa icona di stato viene visualizzata se si rilevano 15 o più incidenti spyware/grayware in un'ora (Worry-Free Business Security (tutti), per impostazione predefinita). Gli amministratori possono modificare la soglia sul server gestito. L'intervallo di un'ora corrisponde ai 60 minuti precedenti al punto di valutazione.
	Questa icona di stato viene visualizzata se si verifica una delle seguenti condizioni: • Lo scanner in tempo reale nel server Exchange è disabilitato. • Un client di protezione non può disinfettare o mettere in quarantena una minaccia informatica. • Per Worry-Free Business Security (Standard o Advanced) 5.1 o versioni successive: Lo scanner in tempo reale è disabilitato su almeno un computer.

Incidenti minaccia virus

Gli incidenti legati a minacce virali corrispondono al numero di rilevamenti di virus o minacce informatiche nel dominio. La console raggruppa queste informazioni statistiche nei seguenti gruppi:

- **Desktop/Server**: virus o minacce informatiche rilevati durante scansioni manuali o quando si accede ai file su computer desktop e server
- **Server Exchange**: virus o minacce informatiche rilevati nei messaggi e/mail elaborati da un server Exchange

Per eventuali informazioni o azioni aggiuntive, fare clic su **Dettagli**.

AVVERTENZA!

Non fare clic su **Reimposta** se non si è certi che gli incidenti siano stati affrontati e contenuti.

Operazione antivirus non riuscita

Gli scanner antivirus eseguono operazioni di disinfezione, messa in quarantena ed eliminazione sui file in cui vengono trovati minacce informatiche o virus. In genere, lo scanner esegue un'operazione iniziale. Se il sistema di scansione non è in grado di eseguire una di queste operazioni, fa ricorso a un'operazione secondaria.

Le operazioni non riuscite indicano che un virus o una minaccia informatica è riuscito ad aggirare le difese antivirus e ha infettato il computer. Remote Manager presuppone che i computer per i quali non è riuscita un'operazione di disinfezione, messa in quarantena o eliminazione di virus o minacce informatiche siano infetti.

Per eventuali informazioni o azioni aggiuntive, fare clic su **Dettagli**.

Computer da disinfettare

I computer da disinfettare sono computer che hanno subito un'infezione da virus o minaccia informatica che il client di protezione non è stato in grado di disinfettare, eliminare o mettere in quarantena dopo il rilevamento. In genere, un computer infetto

contiene una copia in esecuzione della minaccia informatica o del virus, che ha configurato il computer in modo da consentire l'avvio e l'esecuzione automatica.

Per visualizzare un elenco dei computer infetti e dei nomi dei virus, fare clic sul numero di computer da disinfettare. Per gestire i computer infetti, implementare Damage Cleanup Services (DCS) nel dominio. Per ulteriori informazioni, fare riferimento a *Comandi di Worry-Free Business Security a pagina 3-27*.

Per gestire i computer che risultano infetti a causa di operazioni antivirus non riuscite, implementare Damage Cleanup Services (DCS) nel dominio. Per ulteriori informazioni, fare riferimento a *Comandi di Worry-Free Business Security a pagina 3-27*.

Scansione in tempo reale disattivata

I computer nei quali è disattivata la funzione di scansione in tempo reale non sono in grado di esaminare i file non appena arrivano o vengono elaborati. Questi file tuttavia saranno comunque analizzati all'avvio della scansione pianificata. Questi computer sono particolarmente suscettibili alle infezioni di virus o minacce informatiche. I server Exchange su cui la scansione in tempo reale è disattivata permettono il passaggio di tutti i file (anche quelli contenenti minacce informatiche) nei messaggi e-mail, lasciando la rete del cliente vulnerabile ai worm di invio di posta di massa.

Per eventuali informazioni o azioni aggiuntive, fare clic su **Dettagli**.

Per attivare lo scanner in tempo reale su tutti i computer e i server Exchange nel dominio, selezionare il cliente e fare clic su **Risolvi**.

Dettagli sullo stato anti-spyware

Nota

L'anti-spyware è disponibile solo per Worry-Free Business Security (tutti).

Per visualizzare lo stato anti-spyware, nella pagina **Clienti** vengono visualizzati icone di stato e colori che indicano un tasso di incidenti di spyware/grayware relativamente alto e la presenza di computer infetti da spyware/grayware.

Nella tabella riportata di seguito sono descritte le possibili icone di stato anti-spyware.

Tabella 9-3. Icone di stato anti-spyware

Icona di stato	Descrizione
	Sono stati rilevati 15 o più incidenti spyware/grayware in un'ora (Worry-Free Business Security (tutti), per impostazione predefinita). È possibile modificare la soglia sul server gestito. L'intervallo di un'ora corrisponde ai 60 minuti precedenti al punto di valutazione.
	Operazione richiesta. Almeno un computer deve essere riavviato per rimuovere completamente un'infezione da spyware/grayware.

Richiesto riavvio del computer per Anti-spyware

Nella schermata di richiesta di riavvio del computer per anti-spyware viene visualizzato il numero di computer infetti da spyware/grayware che sono stati disinfettati in modo parziale. Questi computer rimangono infetti perché lo spyware/grayware che li ha colpiti non può essere rimosso completamente fino a quando non si riavviano i computer. Per completare il processo di disinfezione su questi computer, contattare un amministratore presso la sede del cliente e chiedere di riavviare i computer manualmente.

Per eventuali informazioni o azioni aggiuntive, fare clic su **Dettagli**.

AVVERTENZA!

Non fare clic su **Reimposta** se non si è certi che gli incidenti siano stati affrontati e contenuti.

Incidenti minaccia spyware/grayware

Gli incidenti legati a minacce di spyware/grayware corrispondono al numero di rilevamenti di spyware/grayware nel dominio. Per visualizzare l'elenco dei computer interessati e dei nomi delle minacce di spyware/grayware, fare clic sul numero di incidenti. Per azzerare il conteggio corrente, fare clic su **Reimposta**.

Per eventuali informazioni o azioni aggiuntive, fare clic su **Dettagli**.

AVVERTENZA!

Non fare clic su **Reimposta** se non si è certi che gli incidenti siano stati affrontati e contenuti.

Dettagli sullo stato anti-spam

La sezione dei dettagli sullo stato anti-spam avverte del numero crescente di messaggi di spam elaborati dal server Exchange. La schermata visualizza icone di stato per mostrare se la percentuale dei messaggi di spam (rispetto a tutti i messaggi elaborati dai server Exchange) ha raggiunto una determinata soglia. Un evento anti-spam viene visualizzato nel pannello di controllo solo se si è verificato almeno un evento di questo tipo.

Nella tabella seguente sono riportate le possibili icone di stato.

TABELLA 9-4. Icone di stato anti-spam

ICONA DI STATO	DESCRIZIONE
	Attenzione. I messaggi di spam sono più o pari al 10% dei messaggi totali elaborati dal server Exchange server (Client Server Messaging/Worry-Free Business Security Advanced, per impostazione predefinita). Gli amministratori possono modificare la soglia sul server gestito.
	Questa icona non viene utilizzata per mostrare tali dettagli.

Dettagli sullo stato dei virus di rete

La sezione dei dettagli sullo stato dei virus di rete segnala attività significative di virus sulla rete. Nella schermata Gestione evento vengono visualizzate icone di stato associate a colori per indicare se l'attività dei virus di rete nei domini del cliente ha raggiunto una determinata soglia. Nel pannello di controllo viene visualizzato un evento virus di rete solo se nella rete si verifica almeno un evento virus.

TABELLA 9-5. Icone di stato dei virus di rete

ICONA DI STATO	DESCRIZIONE
(avviso)	Questo è un messaggio di avviso. Sono stati rilevati dieci o più incidenti legati a virus di rete in un'ora (Worry-Free Business Security (tutti), per impostazione predefinita). Gli amministratori possono modificare la soglia sul server gestito. L'intervallo di un'ora corrisponde ai 60 minuti precedenti al punto di valutazione.
(errore)	Questa icona non viene utilizzata per mostrare tali dettagli.

Per eventuali informazioni o azioni aggiuntive, fare clic su **Dettagli**.

Dettagli sullo stato di Web Reputation

Reputazione Web valuta il potenziale rischio per la sicurezza delle pagine Web richieste prima di visualizzarle. In base alla classificazione restituita dal database e al livello di sicurezza configurato, Client/Server Security Agent, presente nei computer gestiti da Worry-Free Business Security (tutti), blocca o approva la richiesta. La sezione Web Reputation Services indica il numero di tentativi di recupero delle pagine Web classificate come pericolo per la sicurezza. Nel pannello di controllo viene visualizzato un evento Web Reputation solo se si verifica almeno un evento di questo tipo.

TABELLA 9-6. Icone di stato di Web Reputation

ICONA DI STATO	DESCRIZIONE
(avviso)	Sui client vengono rilevati numerosi o frequenti violazioni degli URL. Sono state rilevate più di 200 violazioni in 1 ora (Worry-Free Business Security (tutti), per impostazione predefinita). Gli amministratori possono modificare la soglia sul server gestito. L'intervallo di un'ora corrisponde ai 60 minuti precedenti al punto di valutazione.
(errore)	Questa icona non viene utilizzata per mostrare tali dettagli.

Dettagli sullo stato di monitoraggio del comportamento

Monitoraggio del comportamento monitora il client che tenta di apportare modifiche al sistema operativo e ad altri programmi. Quando un Client/Server Security Agent installato su computer gestiti da Worry-Free Business Security (tutti) rileva un tentativo, invia all'utente una notifica della modifica. A questo punto, l'utente può consentire o bloccare la richiesta. Gli amministratori o gli utenti di Worry-Free Business Security (tutti) possono creare degli elenchi di eccezioni per consentire a determinati programmi di funzionare, pur effettuando una modifica monitorata, o per bloccare completamente determinati programmi. Quando il numero di violazioni supera la soglia, l'icona di stato cambia e il numero di incidenti viene elencato nel **pannello di controllo** e nella schermata **Gestione evento**.

TABELLA 9-7. Icone di stato di Web Reputation

ICONA DI STATO	DESCRIZIONE
	Sui client vengono rilevati numerosi o frequenti violazioni degli URL. Sono state rilevate più di 200 violazioni in 1 ora (Worry-Free Business Security (tutti), per impostazione predefinita). Gli amministratori possono modificare la soglia sul server gestito. L'intervallo di un'ora corrisponde ai 60 minuti precedenti al punto di valutazione.
	Questa icona non viene utilizzata per mostrare tali dettagli.

Dettagli sullo stato dei filtri URL

Il modulo per il filtraggio degli URL fornisce strumenti potenti ed efficaci per gestire l'accesso a Internet dei dipendenti e bloccare i siti Web offensivi o non attinenti al lavoro. Questo modulo filtra i contenuti attraverso un database contenente milioni di URL suddivisi per categorie e utilizza la tecnologia di classificazione dinamica per classificare nuove pagine Web, in tempo reale o in background. I manager IT possono impostare criteri di URL per gruppo o utente, categoria, tipo file, ora, giorno, larghezza di banda e altre variabili.

Nota

Il modulo per il filtraggio degli URL è disponibile solo per Worry-Free Business Security Services e Worry-Free Business Security Standard e Advanced 6.0 e versioni successive.

TABELLA 9-8. Icone di stato dei filtri URL

ICONA DI STATO	DESCRIZIONE
	Attenzione. Il numero di eventi di filtraggio degli URL è maggiore di 300 nell'ultima ora.
	Questa icona non viene utilizzata per mostrare tali dettagli.

Dettagli sullo stato di Controllo dispositivi

Il modulo Controllo dispositivi include strumenti potenti ed efficaci per controllare l'accesso a dispositivi di memorizzazione esterni e risorse di rete.

Nota

Il modulo Controllo dispositivi è disponibile solo per Worry-Free Business Security Standard e Advanced 7.x e versioni successive.

TABELLA 9-9. Icone di stato di controllo dei dispositivi

ICONA DI STATO	DESCRIZIONE
	Attenzione. Il numero di incidenti legati all'accesso a dispositivi non autorizzati è stato superiore a 300 nell'ultima ora.
	Questa icona non viene utilizzata per mostrare tali dettagli.

Smart Scan

Trend Micro™ Worry-Free Business Security si avvale della nuova tecnologia Smart Scan. Precedentemente, i client Worry-Free Business Security Services utilizzavano solo la scansione tradizionale, in base alla quale ciascun client scaricava componenti legati alla scansione. Con il processo Smart Scan, invece, il client utilizza il file di pattern su Smart Protection Server. Per la scansione dei file vengono utilizzate solo le risorse di Smart Protection Server.

Nota

La tecnologia Smart Protection viene applicata solo a Worry-Free Business Security Standard e Advanced versioni 6.x e successive, e Worry-Free Business Security Services 3.x e versioni successive.

TABELLA 9-10. Icone dello stato dell'uso del disco

ICONA DI STATO	DESCRIZIONE
	Smart Protection Service è stato interrotto su un Agent Worry-Free Business Security.
	Smart Protection Service è stato interrotto su un Agent Worry-Free Business Security.

Se Smart Protection Service non è in esecuzione, attendere 30 minuti per consentire all'Agent di sincronizzarsi con il server di scansione globale. Se l'Agent non effettua ancora la connessione al server di scansione globale, controllare la connessione a Internet dell'Agent. Per ulteriore assistenza, contattare il fornitore del supporto.

Aggiornamento dei componenti

Nella tabella riportata di seguito sono illustrate le icone visualizzate nella pagina **Cliente** per indicare eventuali problemi di aggiornamento.

TABELLA 9-11. Icone di stato dell'aggiornamento

ICONA DI STATO	DESCRIZIONE
	Attenzione. Questa icona di stato viene visualizzata se si verifica una delle seguenti condizioni: • Il prodotto gestito non è stato aggiornato correttamente per più di sette giorni. • Il rapporto di implementazione del motore e del pattern su computer desktop e server è inferiore al 90%.

ICONA DI STATO	DESCRIZIONE
✖	Operazione richiesta. Questa icona di stato viene visualizzata se si verifica una delle seguenti condizioni: • Il prodotto gestito non è stato aggiornato correttamente per più di 14 giorni. • Il rapporto di implementazione del motore e del pattern su computer desktop e server è inferiore al 70%. • Almeno un server Exchange è in esecuzione con componenti per la sicurezza non aggiornati.

Per risolvere problemi di aggiornamento, accedere a **Clienti** > **{cliente}** > **Sistema** > **Aggiornamento dei componenti** > **{tipo di prodotto}**, selezionare il prodotto/servizio e fare clic su **Risolvi**.

Dopo avere aggiornato correttamente il server gestito e avere implementato i componenti più recenti, è consigliabile eseguire una scansione manuale (dal menu **Operazioni**). Una scansione è in grado di rilevare minacce ignorate dai componenti obsoleti.

Uso del disco

Nella pagina **Clienti** è possibile monitorare lo spazio su disco dei computer del dominio, visualizzando icone che indicano i problemi di spazio su disco potenziali ed effettivi. Per comprendere il significato di queste icone, vedere la tabella di seguito.

TABELLA 9-12. Icone dello stato dell'uso del disco

ICONA DI STATO	DESCRIZIONE
!	Questa icona non viene utilizzata per mostrare tali dettagli.
✖	Operazione richiesta. Questa icona di stato viene visualizzata se più computer hanno uno spazio su disco inferiore a 1% (1% è il valore predefinito di Worry-Free Business Security Standard e Advanced, che è possibile modificare nella console Worry-Free Business Security Standard e Advanced).

Per risolvere i problemi relativi all'uso del disco, contattare l'amministratore del dominio interessato.

Capitolo 10

Rapporti

In questa sezione sono trattati i seguenti argomenti:

Panoramica sui rapporti

Trend Micro Remote Manager consente di generare, scaricare e inviare rapporti automaticamente. I rapporti forniscono una panoramica relativa allo stato della licenza, ai risultati della valutazione, agli incidenti provocati da minacce, alle minacce principali, nonché ai computer, ai file e agli indirizzi e-mail più colpiti nelle reti dei clienti.

I rapporti includono una varietà di statistiche da Worry-Free Business Security (tutti) e Hosted Email Security. Remote Manager presenta profili rapporto, rapporti singoli e periodici, intervalli di date e vari destinatari e-mail. Remote Manager salva i 30 rapporti giornalieri più recenti, i dieci rapporti settimanali più recenti e i cinque rapporti mensili più recenti. I rapporti generali sono adatti sia per i rivenditori che per i clienti. I rapporti dettagliati sono adatti sia per i rivenditori che per i partner.

Rapporti

Tutti i rapporti

Nuovo rapporto | Elimina | Attiva | Disattiva

Nome rapporto	File	Destinazione	Tipo di rapporto	Frequenza	Ultima generazione	Stato
[PDF]License Report _Daily_WFBS	60	Io	Partner	Giornaliero	14/Apr/2014 16:17:15	
CSV_LR_WFBSS_D aily	25	Io	Partner	Giornaliero	14/Apr/2014 16:17:10	
[CSV]License Report _Daily_WFBSS	60	Io	Partner	Giornaliero	14/Apr/2014 16:17:05	
[CSV]License Report _Daily_WFBS	60	Io	Partner	Giornaliero	14/Apr/2014 14:17:04	
[CSV]Detail Report_ Daily_ALL	60	1	Cliente	Giornaliero	14/Apr/2014 12:17:25	
[PDF]Detail Threat R eport_Daily_ALL	60	1	Cliente	Giornaliero	14/Apr/2014 12:17:18	
[CSV]General Threat Report_Daily_WFBS S	60	1	Cliente	Giornaliero	14/Apr/2014 12:17:13	
[CSV]General Threat Report_Daily_HES	76	1	Cliente	Giornaliero	14/Apr/2014 12:17:13	

Rapporti

Trova rapporto

Utilizza " " per la corrispondenza esatta

Tipo di rapporto

Cliente

Partner

Generato

Tutti

FIGURA 10-1. Pagina Rapporti

I profili rapporto consentono di creare più rapporti a partire da un unico profilo. Ad esempio, è possibile creare un rapporto singolo e generarlo, quindi modificarne alcune opzioni e rigenerarlo senza dover creare nuovamente l'intero rapporto. Attualmente Remote Manager supporta rapporti generali e dettagliati.

Creazione di rapporti

In Trend Micro Remote Manager sono disponibili i seguenti metodi per creare un modello di rapporto:

- Fare clic su un rapporto esistente, modificare il rapporto e fare clic su **Salva** in fondo alla schermata.
- Creare un nuovo modello di rapporto. Per ulteriori informazioni, consultare la sezione *Creazione di modelli di rapporti a pagina 10-3*.

Creazione di modelli di rapporti

Procedura

1. Fare clic sulla scheda **Rapporti** > **Nuovo rapporto**.

   Viene visualizzata la schermata **Nuovo rapporto**.

2. Modificare gli elementi seguenti in base alle necessità.

   - **Nome del rapporto**
   - **Tipo di rapporto**: Per ulteriori informazioni, consultare la sezione *Panoramica sui rapporti a pagina 10-2*.

   I rapporti dettagliati sono disponibili solo per Worry-Free Business Security.

3. Selezionare l'**intervallo di date** del rapporto:

   - **Rapporto singolo**

Opzione	Descrizione
Oggi	Calcola il rapporto con i dati ricevuti dalla mezzanotte fino al momento della generazione del rapporto (in base al fuso orario selezionato). **Nota** Il fuso orario del rapporto è quello selezionato dal rivenditore durante la creazione del profilo. Non viene determinato dal computer del cliente.
Ultimi 7 giorni	Calcola il rapporto con i dati relativi agli ultimi 7 giorni (esclusa la data attuale).
Ultimi 30 giorni	Calcola il rapporto con i dati relativi agli ultimi 30 giorni (esclusa la data attuale).
Intervallo specifico	La data "Da" deve essere successiva o uguale alla prima data dell'ultimo mese (Remote Manager memorizza soltanto i dati dell'ultimo mese e di quello in corso). La data "A" deve essere precedente o uguale a quella attuale.

- **Rapporto ricorrente**

Opzione	Descrizione
Rapporto giornaliero	La data di fine deve essere precedente alla data del giorno corrente. Ogni giorno, definito nell'intervallo specificato, viene generato un rapporto in base ai dati del giorno precedente. Ad esempio, se l'intervallo va dal 27/01/2009 al 29/01/2009: • Il giorno 27, Remote Manager genera un rapporto basato sui dati del giorno 26 • Il giorno 28 Remote Manager genera un rapporto basato sui dati del giorno 27 • Il giorno 29 Remote Manager genera un rapporto basato sui dati del giorno 28

Opzione	Descrizione
Rapporto settimanale	Remote Manager genera il rapporto settimanale ogni lunedì utilizzando i dati della settimana precedente. Di conseguenza, se si desidera generare un rapporto relativo alla settimana in corso, è necessario impostare come data di fine almeno il lunedì della settimana successiva.
Rapporto mensile	Remote Manager genera il rapporto mensile ogni secondo giorno del mese utilizzando i dati del mese precedente. Di conseguenza, se si desidera generare un rapporto relativo al mese in corso, è necessario impostare come data di fine almeno il secondo giorno del mese successivo.

4. Definire le impostazioni di **Contenuti del rapporto**. È possibile impostare i seguenti elementi:

Opzione	Descrizione
Formato rapporto	Formato PDF o CSV
Lingua rapporto	La lingua del rapporto.
Logo	Il logo è facoltativo. Il logo del partner deve essere un'immagine `.png`, `.jpg`, `.bmp` o `.gif` con dimensioni consigliate di 600 x 55 pixel (larghezza x altezza).
Nota	il campo Nota è destinato a uso interno e non viene visualizzato sul rapporto.

5. Fare clic su **Avanti**.

6. Selezionare la data del rapporto. Selezionare un modello di rapporto e la data da generare.

Nota

Se il rivenditore non è connesso al server del cliente e non sono disponibili dati, per il cliente non vengono visualizzate informazioni.

7. Fare clic su **Avanti**.

8. Selezionare i clienti che generano il rapporto.

Nota

È possibile fare clic su **Fine** per generare i rapporti per i clienti selezionati.

9. Specificare i dettagli del rapporto e-mail. I destinatari presenti nelle opzioni **E-mail** provengono dall'elenco dei contatti delle aziende. Vedere *Aggiunta di contatti a pagina 5-9*. È inoltre possibile aggiungere gli indirizzi e-mail che ricevono i rapporti generati.

Nota

Per ciascun cliente selezionato sono disponibili vari destinatari e-mail. È possibile aggiungere o eliminare i destinatari e-mail oppure un logo a seconda dei clienti.

10. Fare clic su **Fine**.

    Il modello di rapporto viene aggiunto all'elenco di quelli disponibili.

Visualizzazione dei rapporti

Per poter essere visualizzato, un rapporto deve essere stato generato almeno una volta.

Accedere a **Rapporti** > **{nome rapporto}** > **File dei rapporti (scheda)** > **{file nel menu Visualizza}**.

Per ulteriori informazioni, consultare la sezione *Panoramica sui rapporti a pagina 10-2*.

Modifica dei rapporti

Accedere a **Rapporti** > **{nome rapporto}**.

Per ulteriori informazioni, consultare la sezione *Creazione di modelli di rapporto a pagina 10-3*.

Download e invio di rapporti

È possibile scaricare e inviare rapporti ai destinatari. Anche se al momento della definizione del rapporto sono stati specificati i destinatari, è possibile modificare l'elenco degli utenti a cui verrà inviato il rapporto.

Procedura

1. Accedere a **Rapporti** > **{elemento o numero di elementi nei file dei rapporti}** > **{rapporto nel menu Visualizza}**.
2. Selezionare i rapporti da inviare o scaricare.
3. Fare clic su **Invia** o su **Download**.

   Per ulteriori informazioni, consultare *Iscrizione ai rapporti a pagina 10-8*.

Iscrizione ai rapporti

Procedura

1. Accedere a **Rapporti** > **{nome rapporto}** > **Pubblico di destinazione (scheda)** > **Aggiungi destinazione**.
2. Selezionare il rapporto del cliente.

Nota

Quando si crea un rapporto, l'elenco dei possibili destinatari e-mail viene ricavato dai dettagli di contatto.

3. Modificare la riga dell'oggetto come desiderato.
4. Fare clic su **Salva**.

Capitolo 11

Risoluzione dei problemi e problemi noti

In questa sezione sono trattati i seguenti argomenti:

Risoluzione dei problemi della console Web Trend Micro Remote Manager

In questa sezione sono trattati i seguenti argomenti:

Problemi di accesso

Impossibile accedere a Trend Micro Remote Manager.

Risoluzione

Le cause di questo problema possono essere due:

- JavaScript è disattivato nel browser. Per Remote Manager è necessario attivare questa opzione. Per istruzioni, consultare la documentazione del browser.
- Il profilo non è stato sincronizzato. Se si è appena eseguita la registrazione su Trend Micro Licensing Management Platform e non si riesce ad accedere, attendere alcuni minuti che avvenga la sincronizzazione delle informazioni.

La struttura di dominio non è visibile dopo l'installazione dell'Agent

La struttura del dominio non è visualizzata nella console fino a quando non si installa l'Agent Remote Manager sul server gestito.

- L'identificatore univoco globale (GUID) non è corretto.
- L'Agent Remote Manager non è in grado di comunicare con Remote Manager.

Risoluzione

1. Assicurarsi che il GUID immesso sia corretto.
   a. Sul server di protezione, utilizzare un editor di testo come Blocco note per aprire il file `C:\Programmi\Trend Micro\WFRMAgentForCSM \AgentSysConfig.xml`.
   b. Verificare il GUID indicato dopo il parametro.

c. Se il GUID è stato corretto, salvare il file e riavviare il servizio Trend Micro Remote Manager Agent.

d. Dopo un paio di minuti, verificare lo stato del dominio del cliente da Remote Manager.

2. Verificare la connessione Agent-server utilizzando la funzionalità Test di connessione.

   a. Accedere a **Start** > **Programmi** > **Trend Micro Remote Manager Agent** > **Agent Configuration Tool**.

   b. Fare clic su **Test di connessione**.

   c. Se il test di connessione non riesce:

      i. Verificare che il server possa connettersi a Internet.

      ii. Verificare che l'indirizzo del server Trend Micro Remote Manager sia stato immesso correttamente.

      iii. Se il server di protezione utilizza un server proxy per la connessione a Internet, è necessario immettere le impostazioni del server proxy.

Impossibile espandere il nodo nella struttura

Se un nodo della struttura del dominio (nella scheda **Clienti**) non si espande a seguito della selezione, è possibile che le informazioni sul gruppo e sul client presenti sul server Worry-Free Business Security e sul server Trend Micro Remote Manager non siano sincronizzate.

Risoluzione

Fare clic sul nodo con il tasto destro del mouse, quindi selezionare **Azione** > **Sincronizza con server gestito** per inviare nuovamente i dati dall'Agent al server Trend Micro Remote Manager.

Impossibile visualizzare la pagina

Il messaggio `Impossibile visualizzare la pagina` viene visualizzato quando si tenta di aprire l'URL del server Trend Micro Remote Manager. Ciò si verifica se:

- L'URL non è corretto.
- L'URL del server Trend Micro Remote Manager non è un sito attendibile di Internet Explorer.

Risoluzione

1. Assicurarsi che l'URL del server Trend Micro Remote Manager sia un sito attendibile di Internet Explorer.
   a. Aprire Internet Explorer.
   b. Fare clic su **Strumenti** > **Opzioni Internet** > **Sicurezza** > **Siti attendibili** > **Siti**.
   c. Controllare che l'URL del server Trend Micro Remote Manager sia nell'elenco. Diversamente, immetterlo e fare clic su **OK**.

Informazioni non corrette nel pannello di controllo

Se il pannello di controllo sembra fornire informazioni incomplete o errate su un particolare dominio, effettuare le seguenti verifiche:

Risoluzione

- Verificare che il server gestito sia stato avviato.
- Verificare se l'Agent è avviato e correttamente in esecuzione.
  - Verificare la console Web Remote Manager in **Clienti (scheda)** > **Tutti i clienti (nella struttura)** > **{cliente}** > **WFBS-S/WFBS-A** > **Dettagli server/Agent (riquadro a destra)** > **Dettagli Agent TMRM** (vedere *Stato dell'Agent a pagina 6-2*).
  - Verificare lo stato dell'Agent sul server gestito (vedere *Gestione degli Agent dal server gestito a pagina 6-6*, *Stato dell'Agent a pagina 6-2* e *Verifica dell'installazione dell'Agent a pagina 4-11*).
- Verificare se il cliente ha reinstallato l'Agent. Verificare inoltre se il cliente ha reinstallato l'Agent utilizzando un GUID diverso o duplicato. Per impostazione predefinita, l'Agent dovrebbe essere aggiornato agli ultimi tre giorni di dati dal server gestito.

- È possibile provare a generare un nuovo GUID e a reinstallare l'Agent.

Impossibile implementare comandi

Se non si è in grado di implementare i comandi di rete in un Agent.

Risoluzione

- Il servizio Worry-Free Business Security (Standard o Advanced) è in esecuzione.
- L'Agent del client è in esecuzione. Diversamente, per avviare l'Agent, vedere *Servizio Agent a pagina 4-11*.
- Le porte 80 e 443 sono aperte. Potete verificarlo eseguendo telnet dal server Remote Manager agli Agent sulle porte 80 e 443, e viceversa. Se le porte non sono aperte, l'amministratore del cliente deve aprire le porte sul firewall.

Stato dell'Agent anomalo

Lo stato anomalo dell'Agent può essere ricollegato a varie cause.

Risoluzione

1. Lo stato dell'Agent sarà anomalo se non invia una richiesta di disconnessione al server Remote Manager prima dell'arresto. Per risolvere questo problema, riavviare il servizio Agent (vedere *Servizio Agent a pagina 4-11*).
2. Se il problema non viene risolto, aprire Agent Configuration Tool facendo clic con il pulsante destro del mouse sull'icona dell'Agent, quindi facendo clic su **Configura**. Fare clic sul pulsante **Test di connessione** per testare la connessione di rete al server Remote Manager.
3. Se si verifica un errore, controllare i criteri del firewall.
4. Se la connessione non presenta problemi, controllare il registro dell'Agent (vedere *Posizione dei registri dell'Agent e dei file di configurazione a pagina 6-13*).

5. Se il problema è serio e tende a ripetersi dopo il riavvio del servizio Agent, attivare il registro di debug (vedere *Attivazione del registro di debug dell'Agent a pagina 6-14*) e contattare il fornitore del supporto.

Funzionamento dell'Agent anomalo utilizzando un GUID esistente dopo...

Perché l'Agent non funziona normalmente usando un GUID esistente dopo aver reinstallato il sistema operativo e l'Agent Remote Manager, aver modificato la scheda di rete del computer o aver installato un Agent su un altro computer?

Risoluzione

Prima di eseguire una delle operazioni sopra citate, è necessario disinstallare l'Agent per eliminare le informazioni esistenti sul server Remote Manager. Se questa operazione non viene eseguita, un Agent che utilizza un GUID esistente non funzionerà in modo corretto.

Risoluzione dei problemi dell'Agent

Problemi dell'Agent

Quando si posiziona il puntatore del mouse sull'icona nella barra delle applicazioni, viene visualizzato un messaggio di stato che indica se l'Agent funziona normalmente o no.

TABELLA 11-1. Messaggi di stato visualizzati dall'icona dell'Agent presente sulla barra delle applicazioni

MESSAGGIO	DESCRIZIONE
Errore sconosciuto. Verificare il sistema e riavviare l'Agent.	Errore sconosciuto. Verificare il sistema e riavviare l'Agent. Errori imprevisti (in genere errori di sistema) impediscono il corretto funzionamento dell'Agent. Risoluzione: Verificare che sul server gestito sia disponibile memoria sufficiente e che non vi siano altri problemi.
Impossibile eseguire la registrazione al server remoto.	Il GUID fornito potrebbe essere sbagliato o potrebbe esserci un problema di rete. Risoluzione Le cause possibili potrebbero essere due: • Verificare di aver utilizzato il GUID corretto. Vedere *GUID dell'Agent a pagina 4-8* per individuare il GUID corretto nella console Web Remote Manager e *Impossibile eseguire la registrazione al server remoto a pagina 11-9* per controllare (ed eventualmente modificare) il GUID sull'Agent. • Se vi è un problema di rete, l'Agent non può collegarsi al server. Controllare la connessione di rete tra il server Worry-Free Business Security (Standard e Advanced) e il server Trend Micro Remote Manager.
Impossibile connettersi al server remoto.	Il server gestito potrebbe riscontrare problemi di connettività Internet. Risoluzione Verificare la connettività Internet sul server gestito. Verificare inoltre le impostazioni proxy dell'Agent e l'indirizzo e la porta del server specificato.

Messaggio	Descrizione
Agent disattivato da Remote Manager.	L'Agent è stato temporaneamente disattivato tramite la console Web Remote Manager. Risoluzione Abilitare l'Agent dalla console Web Remote Manager.
L'Agent non corrisponde alla versione di Client Server Messaging Security (CSM).	Le versioni di Client Server o Client Server Messaging Security Suite e Agent non corrispondono. Risoluzione Aggiornare il server Client Server o Client Server Messaging Security Suite all'ultima versione e installare l'Agent più recente.
Servizio Agent arrestato.	L'Agent è stato disconnesso da Remote Manager. Risoluzione Avviare il servizio dell'Agent facendo clic con il pulsante destro del mouse sull'icona dell'Agent sulla barra delle applicazioni e selezionando **Avvia servizio**.
Impossibile caricare i componenti. Potrebbe essere necessario reinstallare l'Agent.	L'Agent ha riscontrato problemi durante il caricamento di alcuni componenti. Risoluzione Riavviare il servizio dell'Agent facendo clic con il pulsante destro del mouse sull'icona dell'Agent sulla barra delle applicazioni e selezionando **Riavvia servizio** o **Avvia servizio**. Se non funziona, disinstallare e quindi reinstallare l'Agent. Assicurarsi di utilizzare lo stesso GUID.

Impossibile connettersi al server

Quando si fa clic sul pulsante Test di connessione nell'Agent Configuration Tool di Trend Micro Remote Manager e viene visualizzato il messaggio `Impossibile connettersi al server. Le impostazioni potrebbero non essere valide. Immettere impostazioni valide e riprovare.`

Risoluzione

Provare una delle correzioni riportate di seguito:

- Il server gestito non riesce a connettersi a Internet. Accertarsi che Worry-Free Business Security Advanced sia in grado di accedere a Internet.
- Il valore FQDN del server di comunicazione Remote Manager non è corretto. Utilizzare il valore FQDN corrispondente alla propria zona:
    - `Asia Pacifico`: `rm-apaca.trendmicro.com`
    - `Europa e Medio Oriente`: `rm-emeaa.trendmicro.com`
    - `Giappone`: `rm-jpa.trendmicro.com`
    - `America Latina`: `rm-lara.trendmicro.com`
    - `Nord America`: `rm-usa.trendmicro.com`
- Se il server di protezione utilizza un server proxy per la connessione a Internet, assicurarsi che le impostazioni proxy e di autenticazione utente siano configurate correttamente.

Impossibile eseguire la registrazione al server remoto

Il messaggio `Impossibile eseguire la registrazione al server remoto` viene visualizzato quando si sposta il puntatore del mouse sull'icona dell'Agent Trend Micro Remote Manager.

Risoluzione

Ciò si verifica quando l'identificatore univoco globale (GUID) non è corretto. Per risolvere il problema:

1. Accedere a `<install path>\Trend Micro\WFRMAgentForCSM`.
2. Aprire il file `AgentSysConfig.xml` utilizzando un editor di testo.
3. Cercare il GUID tra i parametri "`<AgentGUID>`" e "`</AgentGUID>`".
4. Modificare il GUID e salvare il file.

5. Nella stessa cartella, aprire il file `csmSysConfig.xml` utilizzando un editor di testo.

6. Cercare il GUID tra i parametri "`<ProductGUID>`" e "`</ProductGUID>`".

7. Modificare il GUID e salvare il file.

8. Fare clic destro sull'icona dell'Agent Trend Micro Remote Manager sulla barra delle applicazioni, quindi fare clic su **Riavvia servizio**.

Problemi di connessione con Hosted Email Security

Se la connessione a o la disconnessione da Hosted Email Security si conclude con un errore, è possibile che in fondo alla pagina venga visualizzato uno dei seguenti messaggi:

MESSAGGI	RISOLUZIONE
Impossibile connettersi al server Remote Manager. Controllare la connessione di rete e lo stato di Remote Manager.	Controllare la connessione di rete e lo stato di Remote Manager, quindi riprovare.
Chiave di autorizzazione non valida	Verificare il GUID. Se il GUID è errato, eliminare l'Agent e tentare di nuovo la connessione.
Chiave di autorizzazione duplicata	Verificare il GUID. Se il GUID è errato, eliminare l'Agent e tentare di nuovo la connessione.
Impossibile connettersi al server Remote Manager di Remote Manager. Verificare la connessione di rete e lo stato del server Remote Manager.	Controllare la connessione di rete e lo stato di Remote Manager, quindi riprovare.
Errore interno del server	Contattare il fornitore del supporto.

Problemi noti del server

Di seguito sono riportati alcuni problemi noti del server in questa release.

Icone di stato non coerenti

Nelle fasi iniziali della raccolta dati (immediatamente dopo la registrazione dell'Agent nel server) Remote Manager può visualizzare icone di stato antivirus e anti-spam non coerenti con il numero visualizzato di virus e spam.

Immediatamente dopo la registrazione nel server, l'Agent trasmette gli stati antivirus e anti-spam correnti da Worry-Free Business Security (tutti), ma non i dati cronologici sui quali si basano tali stati. Di conseguenza, potrebbe visualizzare, ad esempio, un simbolo di stato rosso che tuttavia non corrisponde ad alcun incidente visualizzato.

Risoluzione

Remote Manager visualizza l'icona e i dati corretti non appena Worry-Free Business Security (tutti) rileva un incidente.

Dati di spam non coerenti con Worry-Free Business Security Standard o Advanced

I dati spam di Worry-Free Business Security Standard o Advanced e Remote Manager potrebbero non corrispondere se i server che eseguono entrambi i sistemi si trovano in zone con fusi orari differenti.

Risoluzione

Gli incidenti di spam nella console Web Remote Manager e nei rapporti potrebbero avere date precedenti o successive, in base alla differenza temporale tra i server.

Nome utente non corretto sulla console Worry-Free Business Security Services

Dopo aver eseguito l'accesso a Worry-Free Business Security Services mediante la console Web Remote Manager, su quest'ultima viene visualizzato il nome del rivenditore invece del nome del cliente.

Risoluzione

Attualmente non è disponibile alcun metodo di risoluzione di questo problema.

Informazioni di licenza non coerenti nella console Worry-Free Business Security Services

Quando un rivenditore modifica le informazioni di licenza sulla console Web Remote Manager in risposta a un evento relativo alle licenze, l'avviso non cambia fino a che non avviene la sincronizzazione con Remote Manager.

Risoluzione

Attendere circa cinque minuti per consentire la sincronizzazioni di Worry-Free Business Security Services con Remote Manager.

Non è possibile accedere contemporaneamente a due schede o finestre dello stesso browser

Se un rivenditore tenta di accedere più volte da un'altra scheda o finestra dello stesso browser, viene indirizzato automaticamente alla scheda o alla finestra aperta.

Risoluzione

Disconnettersi dalla sessione iniziale prima di avviare una nuova sessione.

I rapporti cronologici vengono eliminati automaticamente

È possibile modificare solo il numero massimo di rapporti giornalieri memorizzati da Remote Manager. Una volta raggiunta la quota, i rapporti precedenti vengono eliminati automaticamente.

Risoluzione

Si consiglia di scaricare i rapporti precedenti su computer o su altri dispositivi di archiviazione.

Non è possibile gestire un account Worry-Free Business Security Services scaduto

Remote Manager non visualizza le informazioni relative ad account Worry-Free Business Security Services scaduti, in quanto Worry-Free Business Security Services elimina i dati sugli account obsoleti.

Risoluzione

Si consiglia di rinnovare gli account Worry-Free Business Security Services quando richiesto.

Connessione ConnectWise interrotta

La connessione ConnectWise con un cliente viene interrotta se si aggiorna l'ID dell'azienda in ConnectWise.

Risoluzione

Nella schermata Remote Manager Customer di ConnectWise, aggiornare il nuovo ID dell'azienda.

Problemi noti dell'Agent

Di seguito sono riportati alcuni problemi noti dell'Agent in questa release.

La reinstallazione degli Agent provoca sovrapposizione di dati

Al momento della registrazione, gli Agent trasmettono automaticamente tre giorni di dati Worry-Free Business Security (tutti). Se un Agent viene disinstallato e reinstallato nell'arco di tre giorni, probabilmente provocherà una sovrapposizione di dati.

Risoluzione

Eseguire il backup dei file di configurazione dell'Agent prima di rimuovere l'Agent e ripristinare questi file dopo aver reinstallato l'Agent. Per ulteriori informazioni, fare riferimento a *Backup e ripristino delle impostazioni dell'Agent a pagina 6-11*.

I risultati del comando di scansione non possono essere verificati

L'Agent non è in grado di verificare se Worry-Free Business Security Standard o Advanced esegue correttamente il comando di scansione nella rete. Questo impedisce a Remote Manager di verificare i risultati del comando di scansione.

Risoluzione

Potrebbe essere necessario verificare lo stato del comando di scansione attraverso l'amministratore IT del cliente.

Agent Configuration Tool non visibile dopo l'aggiornamento dell'Agent

Agent Configuration Tool non è visibile dopo l'aggiornamento dell'Agent su un sistema operativo Windows Vista™ o Windows Server 2008™. Prima dell'aggiornamento, di solito l'utente esegue Agent Configuration Tool dal suo account utente. Durante il processo di aggiornamento, lo strumento viene interrotto e successivamente viene riavviato da LocalSystem, anziché dall'account utente. Per questo motivo, pur essendo in esecuzione, l'utente non è in grado di vederlo.

Risoluzione

È necessario riavviare il computer per riavviare Agent Configuration Tool all'interno dell'account utente.

Domande frequenti

Domande frequenti sulle console Web

Perché l'Agent indica la versione 1.6 nella console Remote Manager e la 3.2 nel server Remote Manager?

Remote Manager 3.2 utilizza ancora l'Agent 1.6 (sui server precedenti a WFBS 6.0). Solo il server è della versione 3.2.

Un rivenditore può disporre di più account per Remote Manager?

No. Per Remote Manager 3.1, un rivenditore può disporre di un solo account.

Se si seleziona Hosted Email Security nell'elenco "Visualizza per" sopra la struttura clienti, perché la struttura continua ad essere ordinata per nome cliente?

Se si seleziona Hosted Email Security, viene applicato un filtro che mostra tutti i clienti Hosted Email Security; non avviene un ordinamento per Hosted Email Security. In altre parole, se si seleziona Hosted Email Security nell'elenco a discesa, vengono visualizzati solo i clienti con Hosted Email Security.

Nota

vengono mostrati anche altri prodotti per questo cliente Hosted Email Security.

Perché alcune voci di menu o opzioni sono disattivate?

È possibile che alcune voci di menu utilizzate per l'invio dei comandi all'Agent risultino disattivate (grigie). Questo può accadere se l'Agent non è stato ancora registrato nel

server Remote Manager o se i dati pertinenti non sono stati ancora comunicati a causa di ritardi nei tempi di rete o altri motivi.

Perché non è possibile modificare la password in Trend Micro Licensing Management Platform?

È probabile che Licensing Management Platform sia in manutenzione. Provare a cambiare la password dopo un po' di tempo. Se il problema persiste, contattare il fornitore del supporto.

È stato appena aggiornato un elemento sulla console, ma lo stato rimane lo stesso. Cosa è potuto accadere?

La sincronizzazione tra servizi richiede alcuni minuti. Alcuni esempi di modifiche ritardate includono l'aggiornamento di licenze e postazioni, la reimpostazione dei contatori e così via.

Sulla console non è visualizzato un servizio Worry-Free Business Security Services del cliente. Perché?

Se sono trascorsi 60 giorni dalla scadenza del servizio, questo non viene visualizzato.

Dopo aver fatto clic sul collegamento per accedere a Worry-Free Business Security Services, viene visualizzato un errore. Perché?

Ciò accade se Worry-Free Business Security Services non è attivo per motivi di manutenzione o se vi sono problemi con Licensing Management Platform. Provare a fare clic sul collegamento dopo un po' di tempo.

Perché un cliente creato in Licensing Management Platform non risulta visibile in Remote Manager?

La sincronizzazione tra servizi richiede alcuni minuti.

Perché l'indicatore "Server gestiti non aggiornati" rimane rosso anche se si fa clic sul pulsante Aggiorna?

Il pulsante **Aggiorna** invia comandi solo al server Worry-Free Business Security Standard o Advanced. Possono verificarsi le seguenti situazioni:

- Il server Worry-Free Business Security Standard o Advanced riceve il comando di aggiornamento. Tuttavia, a causa della configurazione del server Worry-Free

Business Security Standard o Advanced, non è possibile eseguire l'operazione di aggiornamento.

- Il server Worry-Free Business Security Standard o Advanced ha eseguito l'aggiornamento, ma non ha aggiornato la maggior parte dei relativi CSA, quindi continua a inviare un allarme rosso a Remote Manager. Per eseguire l'aggiornamento dei CSA può essere necessario diverso tempo.

Domande frequenti su Hosted Email Security

Perché i dati delle ultime 3 ore non vengono visualizzati nello stato in tempo reale?

Sul server Hosted Email Security, la raccolta dei dati avviene ogni due ore. Per avere la certezza che il server Remote Manager integri i dati del server Hosted Email Security, la raccolta dei dati viene ritardata di 3 ore.

Perché le funzioni Sincronizza con server e Accedi alla console cliente sono disattivate quando si fa clic con il tasto destro del mouse su Hosted Email Security nella struttura clienti?

Le cause per cui Hosted Email Security non è attivo possono essere tre:

- Hosted Email Security non è stato ancora collegato a Remote Manager.
- Il cliente ha interrotto il collegamento. Vedere *Connessione di un cliente Hosted Email Security alla console Remote Manager a pagina 4-14*.
- Probabilmente è necessario aggiornare la struttura clienti.

Perché viene visualizzato il messaggio di errore "Il cliente Hosted Email Security non si è collegato a Remote Manager oppure è stato disconnesso da Hosted Email Security. Contattare l'amministratore" quando si tenta il reindirizzamento alla console Hosted Email Security del cliente dopo che il cliente ha collegato Hosted Email Security a Remote Manager?

Dopo aver inserito il GUID o la chiave di autorizzazione e aver fatto clic su **Connetti**, possono essere necessari anche 10 minuti prima che Hosted Email Security completi il collegamento alla console Web Remote Manager. Se il problema persiste, contattare l'assistenza Trend Micro.

Perché nella console Web Remote Manager, in corrispondenza del codice di attivazione del cliente Hosted Email Security e della data di scadenza, viene indicato "N/D"?

Se un cliente Hosted Email Security non ha collegato il servizio Hosted Email Security a Remote Manager oppure l'ha scollegato, Remote Manager non riesce a recuperare i dati. Un'altra ragione può essere che Hosted Email Security non riesce a individuare un codice di attivazione e una data di scadenza validi per questo cliente. È un caso piuttosto raro.

Domande frequenti sui rapporti

Esiste un limite al numero di rapporti che è possibile archiviare?

Sì. Remote Manager limita il numero dei rapporti archiviati. Una volta raggiunta la quota, i rapporti precedenti vengono eliminati automaticamente. Il numero di rapporti archiviati è il seguente:

- **Rapporti giornalieri**: viene archiviato un massimo di 30 rapporti.
- **Rapporti settimanali**: viene archiviato un massimo di 10 rapporti.
- **Rapporti mensili**: viene archiviato un massimo di 5 rapporti.

Perché non vengono generati rapporti?

Controllare se il disco è pieno. Attualmente Remote Manager offre solo 512 MB di spazio. Provare a scaricare alcuni rapporti sul disco locale, quindi eliminarli dalla console e provare a generare nuovamente i rapporti.

Perché nella cronologia non vi sono nuovi rapporti generati in seguito alla creazione di un profilo rapporti singoli?

Dopo la creazione di un profilo rapporti, è necessario attendere 1 o 2 minuti. A quel punto, il rapporto verrà visualizzato nella cronologia rapporti. Se ancora non è possibile generare il rapporto, aprire il profilo rapporti e salvarlo nuovamente. Se il problema persiste, contattare l'assistenza Trend Micro.

Perché non ricevo rapporti giornalieri/settimanali/mensili via e-mail quando ci sono rapporti nella cronologia?

Verificare che l'indirizzo e-mail del cliente sia valido e che sia stato inserito nell'elenco dei destinatari del profilo rapporti. Se entrambe queste condizioni sono soddisfatte, potrebbe esserci un problema a livello di rete.

Perché nel rapporto generato non viene visualizzata l'ora dei dati con il fuso orario della zona in questione?

Il fuso orario del rapporto è quello selezionato dal rivenditore durante la creazione del profilo. Non viene determinato dal computer del cliente.

Cosa significa N/D dopo la creazione di un rapporto singolo?

Per un rapporto singolo, la colonna dello stato mostra sempre N/D. Ciò accade perché non vi è alcuno stato per il rapporto singolo (non può essere disattivato, attivato, sospeso ecc.).

Perché non è possibile visualizzare i rapporti se si utilizzano connessioni SSL (HTTPS)?

"Non salvare le pagine crittografate sul disco" è un'impostazione di sicurezza per Internet Explorer 7.0/8.0 che viene utilizzata per le connessioni SSL (HTTPS). Se si seleziona questa impostazione, nella cache non viene salvato nulla e non è possibile aprire o scaricare i rapporti.

Per risolvere il problema, in IE 7.0/8.0, fare clic su **Strumenti** > **Opzioni Internet** > **avanzato** > **Sicurezza**e deselezionare "**Non salvare pagine crittografate su disco**".

Capitolo 12

Assistenza

In queste sezioni sono trattati i seguenti argomenti:

Come contattare Trend Micro

In Italia gli addetti Trend Micro sono disponibili via telefono, fax o e-mail:

Indirizzo	TREND MICRO Italy S.r.l. Edison Park Center Viale Edison 110 - Edificio C 20099 Sesto San Giovanni (MI) Italia
Telefono	+39 02 925931
Fax:	+39 02 92593401
Internet	www.trendmicro.it
E-mail	support@trendmicro.com

- Centri di supporto nel mondo:

  http://www.trendmicro.it/informazioni/contatti/index.html

- Documentazione del prodotto Trend Micro:

  http://docs.trendmicro.com/it-it/home.aspx

Semplificazione della chiamata all'assistenza tecnica

Per migliorare il processo di risoluzione dei problemi, è opportuno disporre delle seguenti informazioni:

- Passaggi che hanno causato il problema
- Informazioni sul dispositivo o sulla rete
- Marca e modello del computer ed eventuale hardware aggiuntivo collegato all'endpoint
- Quantità di memoria e spazio libero su disco
- Versione del sistema operativo e del service pack

- Versione client dell'endpoint
- Numero di serie o codice di attivazione
- Descrizione dettagliata dell'ambiente di installazione
- Testo esatto di eventuali messaggi di errore ricevuti.

Utilizzo del portale di supporto

Il portale di supporto Trend Micro è una risorsa online attiva 24 ore su 24, sette giorni su sette, che contiene le informazioni più aggiornate su problemi sia comuni che insoliti.

Procedura

1. Accedere a http://esupport.trendmicro.com.
2. Selezionare un prodotto o servizio dall'elenco a discesa appropriato e specificare qualsiasi altra informazione correlata.

   Viene visualizzata la pagina **Assistenza tecnica**.
3. Per cercare le soluzioni possibili, utilizzare la casella **Cerca assistenza**.
4. Se non si trova alcuna soluzione, fare clic su **Invia caso di assistenza** nel riquadro di navigazione a sinistra e aggiungere uno o più dettagli pertinenti oppure inviare qui un caso di assistenza:

   http://esupport.trendmicro.com/srf/srfmain.aspx

   Il caso viene esaminato da un addetto all'assistenza tecnica di Trend Micro e la risposta giungerà nell'arco di 24 al massimo.

Enciclopedia delle minacce

La maggior parte delle minacce informatiche di oggi è costituita da "minacce miste", ovvero dalla combinazione di due o più tecnologie ideata per bypassare i protocolli di

sicurezza dei computer. Trend Micro è in grado di far fronte a queste complesse minacce informatiche con prodotti che creano una strategia di difesa personalizzata. L'Enciclopedia delle minacce fornisce un elenco completo di nomi e sintomi di varie minacce miste, tra cui le minacce informatiche note, spam, URL dannosi e vulnerabilità riscontrate.

Accedere a http://www.trendmicro.com/vinfo/it/virusencyclo/default.asp per ulteriori informazioni su:

- Minacce informatiche e codice mobile dannoso attualmente attivi o in circolazione
- Pagine informative sulle minacce correlate per creare una cronologia completa degli attacchi Web
- Avvisi sulle minacce Internet riguardo agli attacchi mirati e alle minacce alla sicurezza
- Informazioni sugli attacchi Web e sulle tendenze online
- Rapporti settimanali sulle minacce informatiche.

Informazioni su Trend Micro

Leader globale nell'ambito della sicurezza cloud, Trend Micro sviluppa soluzioni per la protezione dei contenuti Internet e di gestione delle minacce affinché aziende e consumatori di tutto il mondo possano scambiare informazioni in modo del tutto sicuro. Con oltre 20 anni di esperienza, Trend Micro offre le migliori soluzioni client, server e basate su cloud, in grado di bloccare rapidamente le minacce e proteggere i dati in ambienti fisici, virtualizzati e cloud.

Con l'avanzare di nuove minacce e vulnerabilità, Trend Micro continua a impegnarsi per garantire ai propri clienti la sicurezza dei dati, conformità, costi ridotti e salvaguardia dell'integrità aziendale. Per ulteriori informazioni, visitare:

http://www.trendmicro.com

Trend Micro e il logo della sfera con il disegno di una T sono marchi di Trend Micro Incorporated registrati in determinate giurisdizioni. Tutti gli altri marchi di fabbrica e marchi registrati appartengono ai rispettivi proprietari.

TrendLabs

TrendLabs[SM] è una rete globale di centri di ricerca, sviluppo e operativi, impegnati 24 ore su 24, 7 giorni su 7 alla sorveglianza delle minacce, alla prevenzione degli attacchi e a fornire soluzioni tempestive e continuative. Colonna portante dell'infrastruttura del servizio Trend Micro, il personale di TrendLabs è costituito da un team composto da diverse centinaia di tecnici e personale qualificato per l'assistenza, che offre un'ampia gamma di servizi relativi ai prodotti e all'assistenza tecnica.

TrendLabs monitora il panorama delle minacce mondiale per offrire misure di sicurezza efficaci, progettate per rilevare, anticipare ed eliminare gli attacchi. Il culmine giornaliero di questi sforzi viene condiviso con i clienti attraverso frequenti aggiornamenti dei file di pattern dei virus e miglioramenti al motore di scansione.

Ulteriori informazioni su TrendLabs sono disponibili all'indirizzo:

http://cloudsecurity.trendmicro.com/us/technology-innovation/experts/index.html#trendlabs

Indice